Aalto University
School of Engineering

Timo Virtanen

Comparison between safety classification and risk importance measures of systems and components in a nuclear power plant

Thesis submitted as a partial fulfilment of the requirements for the degree of Master of Science in Technology.

Espoo 27.04.2020
Supervisor: Professor Mika Järvinen
Advisor: Lic.Sc. (Tech) Kalle Jänkälä

Aalto-yliopisto
Insinööritieteiden
korkeakoulu

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi

Diplomityön tiivistelmä

Tekijä Timo Virtanen

Työn nimi Ydinvoimalaitoksen järjestelmien ja komponenttien turvallisuusluokituksen ja riskitärkeysmittojen vertailu

Maisteriohjelma Advanced Energy Solutions **Koodi** ENG30

Pääaine Sustainable Energy Conversion Processes **Koodi** ENG3069

Työn valvoja Professori Mika Järvinen

Työn ohjaaja(t) TkL Kalle Jänkälä

Päivämäärä 27.04.2020 **Sivumäärä** 80+6 **Kieli** englanti

Tiivistelmä

Tässä diplomityössä tutkitaan ydinvoimalaitoksen laitteille todennäköisyyspohjaista riskianalyysiä (PRA) hyödyntämällä laskettavia riskitärkeysmittoja ja vertaillaan niiden arvoja laitteiden turvallisuusluokkiin, jotka ovat määritetty perustuen pääosin deterministisiin ohjeisiin suomalaisissa ydinturvallisuusohjeissa. Suomessa on käytössä neljä turvallisuusluokkaa: TL1, TL2, TL3 ja EYT. Useat komponentille asetettavat vaatimukset riippuvat turvallisuusluokasta.

PRA-mallilla mallinnetaan kuinka reaktorin vaurioituminen tai päästön leviämisen estämisen epäonnistuminen riippuu pienemmistä tapahtumista. Mallin tarkimmalla tasolla on kahden eri tyypin tapahtumia: perustapahtumia ja alkutapahtumia. Alkutapahtumat ovat poikkeamia laitoksen normaalista toiminnasta ja jotka vaativat turvallisuustoimintojen käynnistämistä. Perustapahtumat kuvaavat vikaantumisia, jotka mahdollistavat turvallisuustoiminnon epäonnistumisen. Laskentaohjelmistolla voidaan määrittää alku- ja perustapahtumajoukkoja joiden samanaikainen ilmeneminen voi aiheuttaa reaktorin vaurioitumisen ja voidaan laskea sydänvaurioitumistaajuus.

Mallin avulla voidaan myös laskea tärkeysmitat. Vertailuissa käytettiin kolmea eri tärkeysmittaa: Fussell-Veselyä, joka kuvaa osuutta sydänvauriotaajuudesta johon liittyy laitteen vikaantuminen, riskinnousukerrointa, joka kuvaa suhteellista muutosta sydänvauriotaajuudessa kun laite vikaantuu, sekä ehdollista sydänvaurio-todennäköisyyttä, joka on sydänvaurion ehdollinen todennäköisyys kun laite aiheuttaa alkutapahtuman.

Vertailut suoritettiin analysoimalla laitteiden tärkeysmittoja ja turvallisuusluokkia hyödyntäen absoluuttisia arvoja, suhteellisia suuruusjärjestyksiä ja jakaumia. Aikaisempi tieto siitä, että laitteiden turvallisuusluokat eivät ole täysin linjassa niiden turvallisuusluokituksen kanssa, vahvistettiin. Yksittäinen matalan turvallisuusluokituksen laite voi olla tärkeysmittojen mukaan merkittävämpi kuin korkeamman turvallisuusluokituksen laite. Keskimäärin korkean turvallisuusluokan laitteet ovat kuitenkin tärkeämpiä kuin alempien luokkien laitteet. Kullekin turvallisuusluokalle määritettiin ylärajat tärkeysmittojen arvoille, jotka kertovat kuinka suuria tärkeysmittojen arvoja voi kunkin luokan laitteilla olla. Ylärajoja voidaan hyödyntää kun uuden laitteen luokitusta tai vanhan laitteen uudelleenluokitusta harkitaan. Jos yksikin yläraja ylittyy, niin laite tulisi PRA-näkökulmasta luokitella korkeampaan turvallisuusluokkaan.

Avainsanat todennäköisyyspohjainen riskianalyysi, tärkeysmitat, turvallisuusluokitus, ydinvoimalaitos

Aalto University
School of Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi

Abstract of master's thesis

Author Timo Virtanen		
Title of thesis Comparison between safety classification and risk importance measures of systems and components in a nuclear power plant		
Master programme Advanced Energy Solutions		**Code** ENG30
Major Sustainable Energy Conversion Processes		**Code** ENG3069
Thesis supervisor Professor Mika Järvinen		
Thesis advisor(s) Kalle Jänkälä Lic.Sc. (Tech)		
Date 27.04.2020	**Number of pages** 80+6	**Language** English

Abstract

In this thesis risk importance measures (RIMs) calculated for components in a nuclear power plant with probabilistic risk analysis (PRA) are studied and their values are compared to the safety classes given for the components based on primarily deterministic guidelines in Finnish nuclear regulatory guides. There are four safety classes in use: SC1, SC2, SC3 and EYT. Multiple requirements set for a component depend on the safety class.

In nuclear field the PRA models are used to model how the occurrence of smaller events, can lead to core damage or containment failure. Two different types of events can be identified on the highest resolution of a PRA model: basic events (BEs) and initiating events (IEs). IEs are deviations from normal operation that require activation of safety functions and BEs are used to model failures of that can cause the safety functions to fail. PRA-software can then be used to solve sets of IEs and BEs whose simultaneous occurrence can cause core damage and to calculate total core damage frequency (CDF).

The results can also be used to calculate RIMs. Three different RIMs were used in the comparison for components: Fussell-Vesely that measures the share of CDF that involves a failure of the component, Risk Achievement Worth that measures the relative increase in CDF when the component fails and conditional core damage probability that is the probability of core damage given that the component causes an IE.

The comparisons were carried out by analyzing the RIMs and safety classes of components with absolute RIM values, relative rankings and distributions. A previously known fact that RIM values of components are not completely in line with the safety classification was confirmed. A component from a low safety class can be more significant according to RIM values than a component from a higher safety class. However, on average components from a high safety class are considered more significant than components from lower safety classes. Upper limits were determined for safety classes that show how high RIM values can components in each class currently have. The upper limits can be used in assistance when classification of new components or reclassification of existing components is being considered. If any of the upper limits of a safety class are exceeded, then the component should be classified one class higher based on PRA.

Keywords probabilistic risk analysis, importance measures, safety classification, nuclear power plant

Preface

This Master's thesis was conducted at the Nuclear Safety department of Fortum Power and Heat where I started as a summer trainee in the PRA team in May 2019. I want to thank Fortum for the opportunity to write this thesis and the former leader of the PRA team Kalle Jänkälä for the idea for the topic and for acting as the thesis advisor. The topic was an interesting and a very important one. This thesis provided me with an opportunity to learn something new that I previously had little knowledge about. I also want to thank the rest of the PRA team for support and a great working atmosphere.

I want to thank the supervisor of my thesis professor Mika Järvinen who provided me with helpful feedback regarding the formal aspects of writing this thesis and whose lectures I had the joy to attend to during my studies. I also want to thank my family for supporting me on my studies and my friends at the university with whom I studied for six years. The support from peers with whom we faced the same challenges made my years at the university great.

Espoo, 27.4.2020

Timo Virtanen

Table of Contents

Notations

I^{BI}	[1/a]	Birnbaum Importance of a basic event
I^{FV}	[1]	Fussell-Vesely importance of a basic event
I^{RAW}	[1]	Risk Achievement Worth importance of a basic event
J^{BI}	[1]	Birnbaum Importance of an initiating event
J^{CCDP}	[1]	Conditional Core Damage Probability of an Initiating Event
J^{CLRP}	[1]	Conditional Large Release Probability of an Initiating Event
J^{FV}	[1]	Fussell-Vesely importance of an initiating event
K^{FV}	[1]	Fussell-Vesely importance of a component
K^{RAW}	[1]	Risk Achievement Worth of a component
Q	[1]	Probability of a Basic Event
T	[a]	Time interval between test runs
X_i	[1]	Basic Event i
Y_j	[1]	Initiating Event j
Z_k	[1]	Set of Basic Events modelling component k
f_{TOP}	[1/a]	Top event frequency
f_j	[1/a]	Initiating Event frequency
λ	[1/a]	Failure rate
μ	[1/a]	Restoration rate
τ	[a]	Restoration time

Abbreviations

ALARA	As Low As Reasonably Achievable
AOO	Anticipated Operational Occurrence
BE	Basic Event
BI	Birnbaum Importance measure
CCDP	Conditional Core Damage Probability
CDF	Core Damage Frequency
CLRP	Conditional Large Release Probability
DEC	Design Extension Conditions
DIM	Differential Importance Measure
EYT	Non-safety classified (Finn. Ei ydinteknisesti turvallisuus-luokiteltu)
FSAR	Final Safety Assessment Report
FV	Fussell-Vesely importance measure
IAEA	International Atom Energy Association
IE	Initiating Event
KZ-ID	Operating location ID according to AKZ-system
LRF	Large Release Frequency
LO1	Unit 1 of Loviisa nuclear power plant
LO2	Unit 2 of Loviisa nuclear power plant
LOCA	Loss Of Coolant Accident
MCS	Minimum Cut Set
NPP	Nuclear Power Plant
OL	Operating Location
PA	Postulated Accident
PRA	Probabilistic Risk Analysis
RA	Risk Achievement importance measure
RAW	Risk Achievement Worth importance measure
RIM	Risk Importance Measure
RISC	Risk Informed Safety Category
RR	Risk Reduction importance measure
RRW	Risk Reduction Worth importance measure
PWR	Pressurized Water Reactor
SAHARA	Safety As High As Reasonably Achievable
SI	Birnbaum's Structural Importance measure
SC1	Safety Class 1
SC2	Safety Class 2
SC3	Safety Class 3
SC4	Safety Class 4
SSC	System, Structure or Component
STUK	Finnish Radiation and Nuclear Safety Authority (Finn. Säteilyturvakeskus)

1 Introduction

1.1 Background

There were 450 nuclear reactors in operation in the world for generation of power in 2019 and the reactors contributed to around 10 % of the total electricity generation. Nuclear power was also considered the second largest source of low carbon electricity after hydro power. [1] There are four nuclear power reactors in operation in Finland. Two of the reactors are in Loviisa Nuclear Power Plant (NPP) and the other two are in Olkiluoto NPP. In 2019, these four reactor units contributed 25 % of the electricity consumption in Finland [2]. Even with the increasing amount of renewable energy, nuclear power still has an important role in reducing the climate change because of the low emissions of the power generation from nuclear fuel.

The power generation in an NPP is based on a fission chain reaction in which the nucleus of a uranium atom is split into two or more smaller nuclei and neutrons. The energy released from this reaction is used to evaporate water into steam and then the steam is used to rotate a turbine to generate electric energy. The nuclear fuel and the products of a fission reaction are both radioactive and that causes a risk of the radioactive materials being released into the environment. The radioactive materials are primarily stored in the reactor core, but core damage can enable the radioactive materials to escape from the reactor core. After core damage, the radioactive materials can be contained within the plant, but containment failure would allow them to leave the plant.

Due to the risks, the frequencies of their severe consequences must be kept as low as possible. There are many Systems, Structures and Components (SSCs) in an NPP that all have a role in prevention of accidents and mitigating their consequences. The SSCs are safety classified into multiple safety classes in order to categorize them according to their safety significance. The purpose of the safety classification is to allocate resources to the SSCs depending on their safety significance and to secure that the resources are consumed where they are required the most. The safety class guides manufacturing, construction, quality assurance and inspections and testing during operation of an SSC and therefore the costs related to purchase, operation and maintenance for a highly classified SSC can be significantly larger than for an SSC of a lower class. The current classification in Finland and the requirements that a safety class sets for an SSC are both detailed in regulatory guides on nuclear safety (YVL-guides) by the Finnish Radiation and Nuclear Safety Authority (STUK).

Events in which reactor core is damaged and events in which radioactive materials leave the plant after core damage are very rare. Therefore, estimating the frequencies of such events is a complex process. Probabilistic Risk Analysis (PRA) is a methodology that can be applied in NPPs and other complex technological entities to analyze and assess the risks within the technological entities by analyzing sequences of events that can lead to the accident. These sequences are also called accident sequences. The PRA models are used to model how occurrence of smaller events can lead to core damage or containment failure. PRA can be used to produce numerical estimates for risk metrics, including Core Damage Frequency (CDF) and Large Release Frequency (LRF), and to identify the most important accident sequences and SSCs. One method for identifying the most important SSCs is by calculating Risk Importance Measures (RIMs) for the SSCs. The RIMs commonly measure how much

the imperfection of an SSC currently affects the total CDF or LRF, or what are the consequences of the failure of a component.

1.2 Objectives and scope

The safety classes that are primarily based on deterministic guidelines and the RIMs both measure the significance of a component. It is required in guide YVL B.2 [3] that PRA is used in assistance for the safety classification, but more detailed instructions for utilization of PRA are not provided. It is important that the safety classes and RIMs are in line with each other to secure that the most important SSCs have the correct safety class and to secure that resources are not consumed on less important SSCs. Therefore the objectives in this thesis are to study the RIMs, and to compare the RIM values and safety classes of components to each other in order to obtain a justified understanding on the correspondence between safety classes and RIM values and also an understanding about what kind of RIM values can components in each safety class have.

The results from this thesis can be used in assistance of classification of new SSCs and re-classification of current SSCs when modifications are made to the Loviisa NPP. The comparison is limited to the SSCs included in Loviisa PRA model and the results are specific to the Loviisa NPP due to the used data and the PRA model being specific to the plant. Due to the plant being in Finland, this thesis focuses primarily on the Finnish legislation related to safety classification.

Prior studies in Finland on risk-informed safety classification include [4] where a method for risk-informed safety classification was suggested. A comparison between safety classes of component failure events and their RIM values was included in [5] and in this comparison it was concluded that the safety classes are not completely in line with the RIM values and that there is much variance between the RIM values of components in a safety class. The comparison was done on basic event (BE) level and based on the model and data from Olkiluoto NPP operated by Teollisuuden Voima. However, [5] did not include suggestions on the use of RIMs in classification. [5]

1.3 Structure

The structure of this thesis is as follows. The second chapter of this thesis introduces the Loviisa NPP, basics about NPP power generation and safety systems, and relevant aspects about nuclear safety, including safety classification. In the third chapter, the PRA methodology and PRA model contents and quantification are explained. Then, in the fourth chapter, the definitions and calculation of RIMs are explained, the effect of safety class on RIM values is discussed and a foreign application of risk-informed safety categorization is described. The safety classes of SSCs are compared to their RIM values in Chapter 5 and the guiding values are suggested and tested against the current safety classes of components. The sixth chapter concludes this thesis.

2 Nuclear power and nuclear safety

Because this thesis is focused on the Loviisa NPP, this chapter will first introduce the plant. In the second section the power generation systems and other relevant systems of an NPP housing a pressurized water reactor (PWR) are described with the focus on Loviisa NPP. In the third section some aspects of nuclear safety systems are introduced, and the fourth section introduces the safety classification in Finland and some special aspects of safety classification in Loviisa NPP.

2.1 Loviisa nuclear power plant

Loviisa NPP is located on the island of Hästholmen near the Finnish town Loviisa. The plant consists of two units: Loviisa 1 (LO1) and Loviisa 2 (LO2). Construction of LO1 was started in year 1970 and it was connected to grid in 1977. LO2 was constructed after LO1 and it was connected to grid in 1980. Current operating licenses allow operation of LO1 until 2027 and operation of LO2 until 2030. [6]

The Loviisa NPP is a unique mixture of both Western and Eastern technology. The plant was first planned to be purchased as a whole and the supplier was to be selected by competitive bidding. Due to the political climate of the planning phase, the supplier of the main components ended up being chosen to be the Soviet Atomenergoexport. The main components included reactor, turbine and generator. The safety systems were supplied by Western companies for them to comply with the western standards. [7]

Both of the reactors are Soviet-made VVER-440 type (Rus. Водо-водяной энергетический реактор, water-water energetic reactor) PWRs [7]. The reactors both operate at nominal thermal powers of 1500 MW and the net electrical capacities of LO1 and LO2 in 2019 were both 507 MW, resulting in a total 0,338 electrical efficiency of the plant and contribution of 11% of Finland's total electricity production. Total load factor is defined as the ratio between total electricity generation and maximum electrical energy output at constant nominal power and the value for this factor was 93,0% for LO1 in 2019. [8]

2.2 Systems and components in a PWR plant

There are multiple SSCs in a PWR plant. A system is defined in [9] as a functional or structural collection of components assembled to perform a function. Components are equipment, such as pumps, valves, relays or elements of a larger array. Structures are elements, or collections of elements that provide support or enclosure, including buildings, tanks, basins, dikes and stacks. [9] The systems in an NPP can be divided into four groups: process systems, ventilation and heating systems, electrical systems and automation systems. The power generation principle and systems are introduced first, then the safety systems and finally the automation and electrical systems are introduced.

2.2.1 Power generation

The working principle of an NPP is very similar to the one of a conventional power plant. The main difference is the fuel and the reaction with which the thermal energy is released from the fuel. Whereas conventional power plants utilize combustion reaction to release the energy from chemical bonds between atoms, NPPs utilize fission reaction to release the energy from bonds within an atom nucleus. The steam-water cycle of an NPP is illustrated in Figure 1. Next, an overview of the power generation principle of a PWR plant is provided.

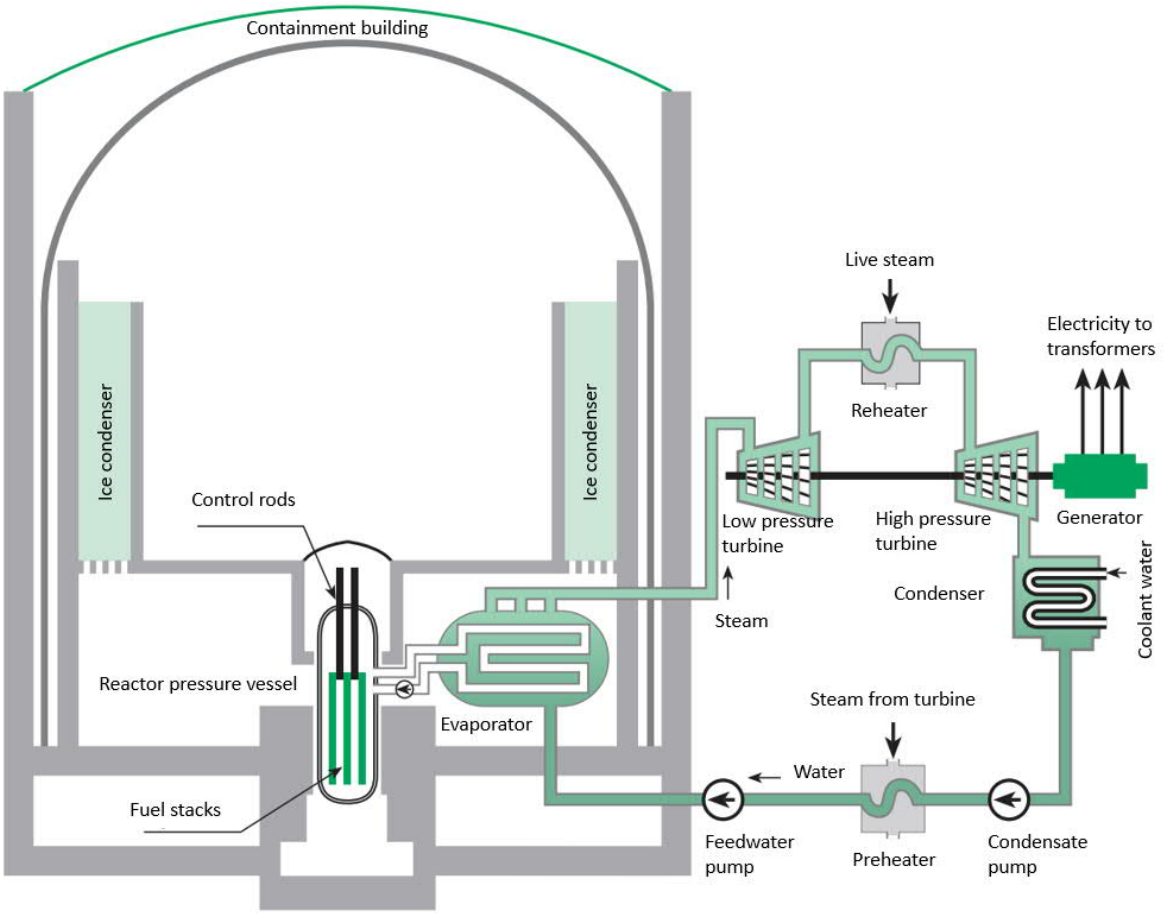


Figure 1 Power generation principle of an NPP. Translated from [7]

Fission reaction and nuclear reactor

The fission reaction is a reaction in which a heavy atom nucleus splits into two smaller nuclei, called fission products, and sub-atomic particles, including neutrons. Energy released in this reaction is released as mostly kinetic energy of the products and is then converted into heat in the interactions between the high velocity products and their surroundings. A VVER-440 type PWR uses uranium oxide as its fuel and the isotope of Uranium is U-235. [10] The fuel is compressed into small ceramic pellets whose diameter is around 1 cm. The pellets are stacked into fuel rods and the rods are assembled into hexagonal fuel stacks. The stacks are surrounded with flow paths for coolant water. [7]

When a U-235 nucleus is bombarded with neutrons, one neutron needs to be absorbed by the nucleus and this initiates the fission reaction. The neutrons released in this reaction are used to initiate the following fission reactions of the other U-235 nuclei and this is called fission chain reaction. Neutrons must be first slowed down in order for them to be able to be absorbed by the other U-235 nuclei. This is done with a moderator, which in a PWR reactor is light water that also serves as reactor coolant to transfer heat out of the reactor. [10] Multiple neutrons are released in one fission reaction and on average only one of those neutrons should initiate a fission reaction for the power output to remain constant. If the average is less than one, the fission chain reaction will eventually end, and the reaction is called subcritical. If the average is more than one, the reaction is called supercritical and the power output keeps increasing. [7]

Reactivity is controlled with control rods and boron concentration of coolant water. Boron is an effective absorbent of neutrons released in the fission reaction. Control rods are located between the fuel bundles and they are moved vertically in the reactor in order to control the reactivity. They are held up with electromagnets and if the current is cut from the magnets, the rods will drop into the reactor to shut it down. [7] The bundles, along with control rods and protective elements form a reactor core. The reactor core is located within a reactor pressure vessel. [11]

Primary coolant circuit
There are two closed coolant circuits in PWR plants: primary and secondary. The primary circuit is used to transfer heat from the reactor to the secondary circuit which is like the water-steam circuit of a conventional power plant. Water in the primary circuit is pressurized to a pressure of 123 bar in order to prevent evaporation and the pressure level is maintained with a pressurizer which contains a mixture of steam and water. To increase the pressure, the mixture is heated with an electric heater to increase the amount of steam and to decrease the pressure, the steam is condensed with water sprays. Primary circuit water is heated in the reactor flow channels within the reactor by the fission reaction. Primary circuit then brings the heated water into evaporators where the heat is transferred into the water of the secondary circuit. The cooled primary circuit water then flows back into the reactor and is heated again. Water flow is maintained with main circulation pumps that pump the water from evaporator into flow channels within the reactor's flow channels. [7] The reactor pressure vessel, pressurizer and the main circuits form the reactor coolant system [11].

Secondary coolant circuit
Secondary circuit water from a feedwater tank is first heated in a preheater with steam from turbine and then fed into the evaporator with feedwater pumps. Water of the secondary circuit is evaporated in the evaporator due to the lower pressure of the secondary circuit. After the evaporator the steam is used to rotate a high-pressure turbine, then it is reheated and mechanically dried and afterwards used to rotate a low pressure turbine. The turbine is connected to a generator shaft whose rotation is used to convert mechanical energy into electrical energy in two generators. After passing through the low-pressure turbine, the steam-water mixture is condensed in a condenser. The heat from the steam-water mixture is transferred to seawater flowing in the seawater circuit. The sea water functions as the ultimate heat sink of the plant where the residual heat is released. [11]

2.2.2 Safety functions and systems

The radioactive materials that are the source of most hazards in an NPP are located for the most part within the fuel pellets and the active materials consist of the fuel and the fission products. The fission products, due to their activity, pose a hazard called decay heat that is the product of the decay of the fission products and it is released even after the fission chain reaction has been stopped. Damage to the reactor can be caused by multiple different kinds of accident sequences, but generally the core is damaged due to a criticality accident, in which the reactor becomes supercritical for an increased amount of the time, or due to a loss of coolant accident (LOCA). Both accidents result in the reactor temperature increasing and possibly damaging it. [12] Definition given for core damage in [13] is:

"uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage is anticipated representing the onset of gap release of radionuclides"

After core damage the active materials can be contained within the plant, but a containment failure may allow a large release to escape the plant. In Finland, a large release is defined as a release of more than 100 TBq of Caesium-137 isotope [14]. LRF is then the mean frequency of a such release. A large early release frequency is defined as the mean frequency of a release of airborne fission products from the containment to the environment before effective implementation of off-site emergency response [13].

Safety functions are utilized in prevention of core damage or containment failure from occurring. They are specific purposes or objectives that must be achieved in order to control the energy sources and radiation hazards in the plant. Systems that are designed for carrying out safety functions are called safety systems. [15] The safety systems of Loviisa NPP are illustrated in Figure 2. In Loviisa NPP the systems were defined before the safety functions were defined. When the plant was being planned, the practices and standards of the time did not include the use of safety functions in assistance of the planning of the plant. [16] Therefore the relationship between specific functions and systems are not that direct in the plant.

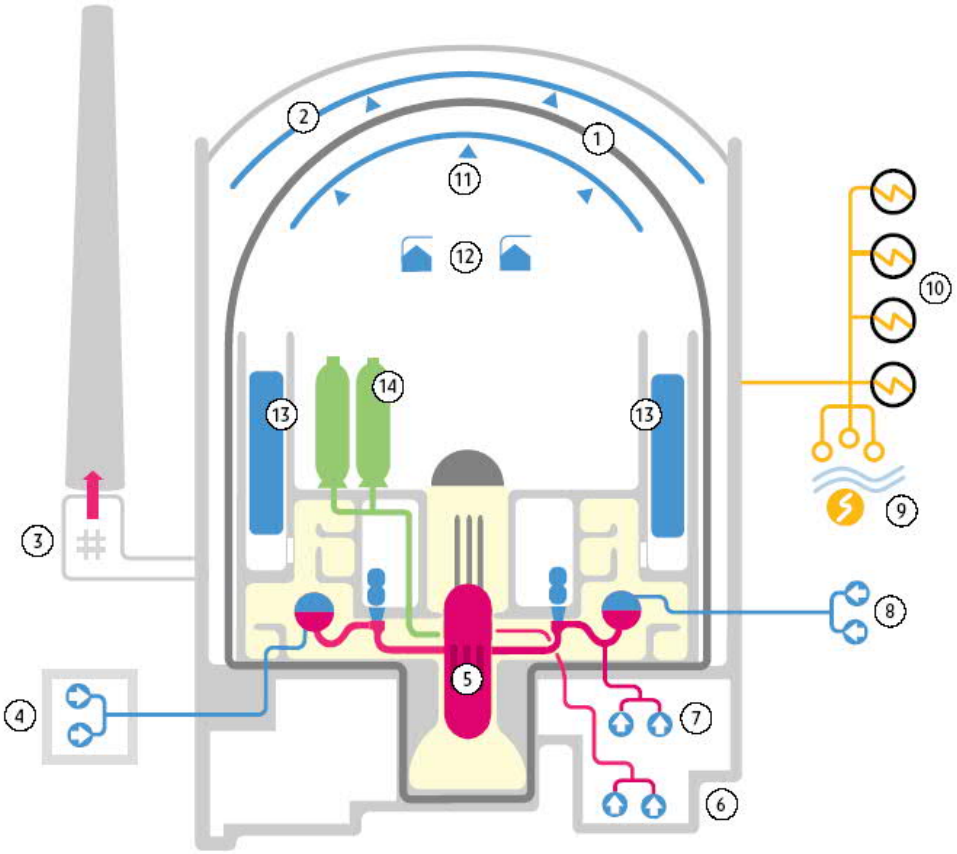


Figure 2 Safety systems in Loviisa NPP. The system numbers are as follows: 1: steel containment, 2: external containment cooling, 3: air filters, 4: additional emergency feed water pumping station, 5: uranium core, 6: low-pressure safety injection pumps, 7: high-pressure safety injection pumps, 8 emergency feed water pumps, 9: power supply from hydropower station, 10: reserve power diesel generators, 11: sprinklers, 12: hydrogen release and recombiners, 13: ice condensers, 14: safety hydro accumulators. Figure from [17]

Identification of safety functions and the systems that carry out the functions is required in Finnish regulation on the safety of a nuclear power plant Y/1/2018 [18]. These functions can be used either for preventing accidents or mitigating their consequences. Safety functions

also have a role in safety classification, and they are used in construction of PRA models. There are three main safety functions identified by International Atomic Energy Agency (IAEA) in [19]:

1. Control of reactivity
2. Removal of heat from the nuclear reactor and from the fuel store
3. Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases

The full list of safety functions is plant specific and more detailed than the list of the main safety functions. In the final safety assessment report (FSAR) of Loviisa NPP [16], these main safety functions along with supporting functions and control of severe accidents are also referred to as safety objectives. The safety objectives are achieved through safety measures and the safety measures are executed with safety functions. [16]

2.2.3 Electrical and automation systems

The electrical systems of Loviisa NPP have three general objectives as described in [20]:

1. Generation of electrical energy
2. Providing electricity to electrical actuators and to automation systems during operation of the plant
3. Providing safety systems with electricity during incidents and accidents

The plant has two connections to the 400 kV grid, one is to the village of Koria and the other is to the village of Anttila. The generators supply the generated electricity through main transformers and switchgear into the grid. The generators, along with the 400 kV connections, are used to supply the SSCs within the plant with electricity during normal operation. During outages, the plant is supplied by a connection to 110 kV grid. The 110 kV connection can be replaced with either a diesel generator, or with a connection to Ahvenkoski hydro power plant. [20]

Both units are also equipped with additional four diesel generators each, two for each redundancy. These generators are used to supply SSCs important to safety with electricity in case the connections to grid are lost. The generators are started up with pressurized air that is stored in pressurized air tanks. Components whose operation cannot withstand the delay in diesel generator startup are supplied with electricity from battery sets. The diesel generators require multiple supporting systems for operation that include startup system, cooling system and fuel systems. [20] While the diesel generators itself are considered electrical systems in this thesis, the supporting systems are considered process systems.

Automation systems are used to control both short term and long-term safety functions in the plant. Short term functions include functions related to normal process control, preventive protection and reactor protection. The long-term functions are related to accident conditions, and the functions are initiated manually. [21] Automation components modelled in the Loviisa PRA model include measurements, automation signals, and automation cabinets and hubs.

2.2.4 Operating locations

The SSCs can be identified by their operating locations (OLs). The OL of a pump does not directly refer to an exact pump, but rather a physical or logical location within a process where the pump operates at. The pump can be moved to storage while another pump is placed in the OL. The pumps also have separate IDs that refer to that exact pump, but the OL is used, for example, in PI-diagrams, PRA models and the OLs are the entities that are safety classified, not the specific pumps. In Loviisa NPP the identification of OLs is based on German AKZ-system that is no longer developed. [22] Figure 3 displays the structure of the KZ-ID of an OL. In this system the OLs form a hierarchy, in which on the top level is the plant unit. The plant unit consists of systems, and the systems consist of subsystems that in turn consist of structures and components. This hierarchy can also be seen in the structure of the KZ-ID as shown in Figure 3.

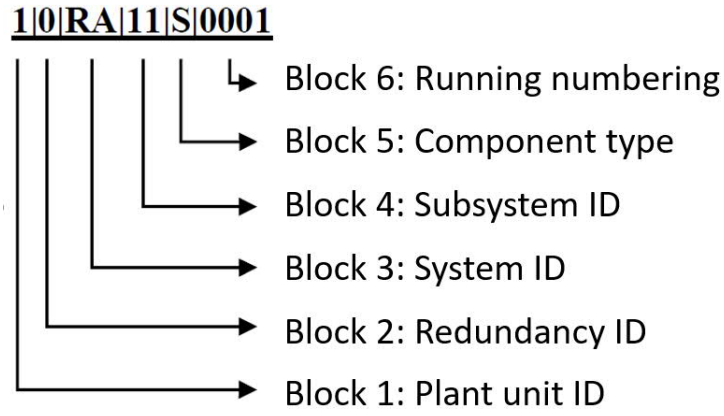


Figure 3 Structure of a KZ-ID used in Loviisa NPP. Translated from [22]

2.3 Nuclear safety

Next some selected aspects about nuclear safety are introduced. These include basic principles applied in Finnish legislation related to nuclear safety, classification of different types of accidents and incidents, and some of the main design principles applied in the safety design of NPPs.

2.3.1 Principles in Finnish legislation

A main principle of Finnish nuclear legislation is that nuclear power, considering all of its impacts, should be beneficial to the society. Utilization of nuclear energy should be safe and not cause damage to people, environment or property. [7] The risks related to nuclear power can always be decreased, but the cost of decreasing the risks increases as the risks are decreased. At some point, the generation from nuclear energy is not beneficial anymore due to the costs of the production. Application of a SAHARA (Safety As High As Reasonably Achievable) principle is required in the Finnish Nuclear Energy Act 990/1987 [23]. This principle requires that all measures should be applied if they can be considered reasonable based on operational experience, safety analyses and development of science and technology [23].

Requirements are set for maximum CDF and LRF values for new plants by STUK in guide YVL A.7 [24]. The upper limit for CDF is defined at $10^{-5}\,\frac{1}{a}$, and the limit for LRF is defined at $5 \times 10^{-7}\,\frac{1}{a}$. [24] In addition to the SAHARA-principle, application of ALARA (As Low

As Reasonably Achievable) principle is required in YVL B.1 [15]. This principle is applied for personnel working in NPPs whose exposure to radioactive materials cannot be removed completely. According to the principle, the plants should be designed so that the personnel's exposure is kept minimal. [15]

2.3.2 Classes of accidents and incidents

Potential accidents and incidents in NPPs are classified depending on the estimated frequency of their occurrence and the radiological release. The classes of accidents for Finnish legislation are described in [14] and upper limits for their radioactive releases are provided. These classes and limitations are primarily used for deterministic analyses and for design requirements of a plant but are also relevant for the deterministic safety classification.

An anticipated operational occurrence (AOO) is a deviation from normal operation that can be expected to occur one or more times during one hundred operating years. [14] AOOs can be caused by a malfunction of a single component for example. AOOs can be coped with by the systems of a plant while having the potential to damage the reactor if other malfunctions are included. [12]

Postulated accidents (PA) are expected to occur less often than once in a hundred years and the plant is expected to withstand them without the fuel being damaged even if individual safety significant components are unavailable due to maintenances or failures. PAs are divided into two classes based on their expected frequency. Class 1 PAs are expected to occur less often than once in a hundred years, but at least once in 1000 operating years. Class 2 PAs are expected to occur less often than once in 1000 operating years. [14]

Design extension conditions (DEC) are an extension to PAs. These accidents are not included in the PAs. DEC refers to three different combinations of different kinds of accidents and failures: [14]

a) accident caused by an AOO or a class 1 PA is accompanied with a common cause failure
b) accident caused by a combination of failures that is identified as significant with PRA
c) accident caused by a rare external event that the plant is expected to withstand without severe fuel damage

A severe accident is an accident in which a significant share of the reactor fuel, or fuel in reactor pool or fuel storage, loses its original structure. Or in other words, core damage occurs. Severe accidents shall not require large precautionary measures of the population, or long-term limitations to land and water areas. [14]

Each class has been set an objective plant state to which the plant should be able to be brought after an accident. These plant states are defined in [18]. There is a controlled state and a safe state. The plant is first brought to controlled state in which the reactor is shut down and decay heat removal is secured. In a safe state the reactor is shut down, depressurized and decay heat removal is secured. For severe accidents, the definitions for controlled and safe state differ a little from other accidents. In controlled state after a severe accident the heat removal from remains of reactor core can be secured, the temperature is constant or decreasing, the remains are in a form that will not become supercritical again and considerable amounts of fission products are not released. In a safe state after a severe

accident the requirements for controlled state are fulfilled and pressure within the confinement building is low enough that amount of leakage is low even if the building has been ruptured. [18]

2.3.3 Design principles

There are multiple requirements and principles related to plant design that are introduced next. These principles have significant impacts on safety as they have an effect on how reliably the systems function. The principles include defence-in-depth, diversity, redundancy and separation -principles.

Defence-in-depth

Defence-in-depth is a fundamental principle applied in the design of NPPs. Application of defence-in-depth is required by IAEA in [25] and in Finnish legislation [23]. Defence-in-depth should be applied in plant design and operation, in all plant states and in all plant operating modes. The main idea of this concept is to provide multiple levels of protection instead of attempting to make one perfect level of protection. If one level would fail, the next one would be available. When this is properly applied, no single human or component failure or external event will lead to harmful consequences. [12] Five levels of defence-in-depth that the plants should be designed to include are identified by IAEA in [18]:

1) Prevention of deviations from normal operation and failures of items important to safety
2) Detection and control of deviations from normal operation in order to prevent AOOs from developing into accident conditions
3) Control of accident conditions resulting from an AOO to prevent them from damaging the reactor core and causing a severe accident
4) Mitigating the consequences of a severe accident by preventing the radioactive release from leaving the plant site
5) Mitigating the radiological consequences of radioactive releases that may result from severe accidents. This includes preparation of on-site and off-site emergency responses for the potential severe accidents

Diversity

Diversity-principle is applied in safety systems to reduce the probability of failure of a whole safety function due to failures that affect multiple components. This is achieved by installing multiple systems or components whose operating principles are different from each other. A common example of this is the control of reactivity. The controlling can be done either with the control rods or by adding boron to coolant water. Diversity-principle is applied also to the control and automation systems in addition to process-systems. Many automation systems function on the basis of measurements and thus it is important to have measurements of different properties, like temperature and pressure. The diversity principle can also be applied on smaller scale by for example purchasing valves from different manufacturers. [7]

Redundancy

Safety systems in NPPs are often divided into multiple redundancies, meaning that there are multiples of parallel and similar SSCs functioning independently of each other. The redundancies are used to reduce the probability that a safety function is unavailable due to individual failures of a components or due to scheduled maintenances. Redundancy requirements for systems and subsystems are presented as fault criterion requirements.

Examples of this include (N+2), (N+1) and (N+0) criteria where N tells the necessary minimum amount of functioning components to achieve the safety function and the number tells how many additional redundant components need to be installed. (N+2) principle means that a safety function must be able to be achieved even if two pumps are out of use due to maintenance or a failure. [7]

Separation
The objective of separation of systems and components is to secure their functionality even in the case a hazard threatens multiple components in a specific location in the plant. For example, these hazards can be a flood or a fire. Separation principle is applied as both physical and functional separation. Physical separation means that the redundant safety systems should be separated in different locations so that the hazard will not prevent both of them from working. Different parts of the power plant process are also located in different buildings. Functional separation means that parallel systems are prevented from interfering with each other. [7]

2.4 Safety Classification

In this section the safety classification legislation and deterministic requirements for safety classification are introduced first. Then some special properties of the classification in Loviisa NPP are introduced. The requirements that a safety class sets are described later in Section 4.4 when their impact on RIM values are discussed.

2.4.1 Safety classification in Finland

It is required in [18] that the SSCs of a Finnish NPP are safety classified according to their safety significance. The safety class of an SSC guides the design, manufacture, installation, operation, inspections and quality assurance of the SSC. [18] The purpose of this is to ensure that the proportion of the listed actions is in line with the safety significance of the SSC. The classification of SSCs in Finland is instructed in more detail in regulatory guide YVL B.2. [3] The latest version of this guide was released in 2019 and the version before that was released in 2013.

The SSCs in an NPP are classified into four classes: 1, 2, 3 and EYT (Finn. Ei Ydinteknisesti Turvallisuusluokiteltu, non-safety classified). The most important SSCs are classified in Safety Class 1 (SC1), while least important components belong to class EYT. There is also a class EYT/STUK for some EYT systems considered important. [3] Special quality requirements are not set by EYT/STUK for the systems, but the class sets additional requirements on information that is required to be delivered to STUK about those systems. The components in EYT/STUK systems generally belong to class EYT. [26] There was also a Safety Class 4 (SC4) that was removed in the 2013 update, while EYT/STUK was added. The purpose of SC4 was to include less important SSCs from higher classes, but it was noticed that more SSCs were moved from class EYT to SC4 than from Safety class 3 (SC3) to SC4. [27]

The classification of SSCs should be based primarily on deterministic methods supplemented by PRA and expert judgement [3]. It is stated in YVL A.7 [24] that PRA should be used during planning phase of a plant to confirm that the safety classes of SSCs are in line with their safety significance. A PRA application should be delivered to STUK with safety classification documentation. During operation phase PRA should be used similarly when there are significant changes made to the plant or PRA model. [24] Neither

of the guides give direct instructions on how PRA should be used in safety classification and there are only direct instructions for deterministic classification in the guide [3]. IAEA also suggests the use of PRA to verify the deterministic safety classification and if there are differences between SSC importance according to PRA and the safety class, then further assessment should be carried out in order to understand the reasons for the deviations [19].

An NPP licensee can diverge from the deterministic requirements stated in YVL B.2 if they can reasonably show that the required safety level is achieved even with another safety class. The approved safety classification of existing components can also be changed to either increase or decrease the safety classification. The application needs to be approved by STUK in both cases. [28]

There are two different safety classes that a component can have: functional safety class and structural safety class. Safety functions and systems can only have the functional safety class and structures can only have the structural safety class. The functional safety class is based on safety functions. The safety functions are classified first based on their significance in prevention of accidents. The functional safety class of a system is then based on the significance of the system in the execution of safety functions. Components that are important for the execution of the safety function of a system generally belong to the same functional safety class as the system. Some components within the system can also belong to higher or lower safety classes. Individual components that are connected to systems of higher safety class can belong to the higher safety class, while components that are less important for the safety functions can belong to a lower safety class. Structural safety class of structures and components is based on the requirements that they have as a barrier against spread of radioactive materials. [3] This includes the requirements in prevention of large pipe leakages, for example [26]. When a component has two different safety classes, the higher one should be used for determining the requirements [3].

The safety classification has its basis in the defence-in-depth principle, but there are no direct connections between safety class and defence-in-depth. Instead, SSCs from multiple different safety classes can be used on the same level of defence-in-depth. [26] The division of safety classes among the defence-in-depth levels is illustrated in Figure 4. Next the deterministic directions for each class are introduced.

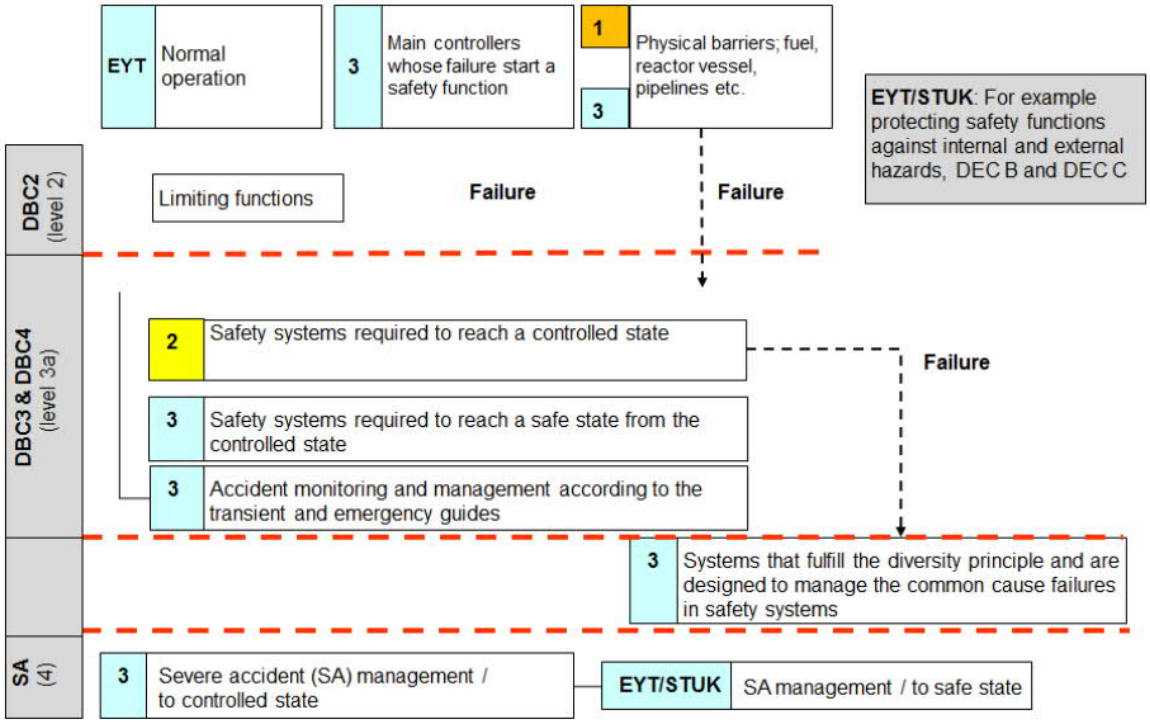


Figure 4 Safety classes and defence in depth. [26]

Safety Class 1

Selected parts of the reactor coolant circuit should be classified as SC1. SC1 is only a structural safety class and it is not used on system-level. On component and structure level this class should include the structures and components whose failure could cause an accident impacting integrity of the reactor and requiring activation of safety measures. This includes nuclear fuel, reactor pressure vessel and the parts of primary circuit whose rupture could result in a primary circuit leak that cannot be replaced with systems related to normal plant operation. [3]

Safety Class 2

Systems and their obligatory support systems should be classified to Safety Slass 2 (SC2) if they are required for executing safety functions related to bringing the plant to controlled state after a PA or if they are required for keeping the plant in the controlled state. Systems that are required for confinement of radioactive materials inside the confinement building after a PA should also be classified to SC2. [3]

Based on the structural requirements, structures and components that should be classified to SC2 include less important parts of the primary circuit and structures and components outside the primary circuit. From the primary circuit SC2 includes pipes and components whose damage can be compensated for with systems related to normal operation, and components that can be isolated from the reactor coolant system with two sequential valves whose closing time is short enough to ensure safe shut down and cooling of reactor. Outside the primary circuit SC2 includes structures and components whose integrity is required for residual heat removal or for confinement after a failure of a SC1 component or after a pipe rupture. In addition, structures and components whose failure endangers the integrity of a SC1 barrier or the nuclear fuel, and whose failure causes a danger of an uncontrollable chain reactor, should be classified to SC2. [3]

According to the asset management system LOMAX [29] that is used in Loviisa NPP, this class includes OLs from a wide range of system groups. These groups include electrical distribution boxes and switchgears, control boards and consoles, fuel systems, secondary circuit, reactor support systems, sea-water circuit, reactor containment, and nuclear steam supply system. [29]

Safety Class 3
The list of conditions based on which systems should be classified to SC3 is much longer than for the higher safety classes. In summary, the list includes systems that are safety-related functionally or structurally, but that are not classified to SC1 or SC2. Based on structural requirements SC3 includes structures that secure SC2 system availability and physical separation, structures and components that secure SC3 safety functions and structures and components related to confinement and handling of radioactive materials, but do not belong to SC1 or SC2 and their failure can lead to significant spread of radioactive materials within the plant or to its surroundings. [3]

Safety Class EYT and EYT/STUK
If the system is not required to be classified into classes 1, 2 or 3, it should be classified into the class EYT (not safety classified). However, the following systems belonging to class EYT should be classified to class EYT/STUK instead: [3]

1. Systems that protect systems in higher safety classes from internal or external events, such as fire extinguishing equipment
2. Systems that are used for monitoring radiation, surface contamination or radioactivity of the plant, but do not belong to SC3
3. Systems that are needed for bringing the plant back to controlled state and from controlled state to safe state after a severe reactor accident

2.4.2 Safety classification in Loviisa NPP

In Loviisa NPP the SSCs are classified according to YVL B.2 but there are some special aspects about the classification. While it is described in YVL B.2 that a single component can have up to two safety classes, the SSCs in Loviisa NPP can have up to four different safety classes. A single valve can have a functional safety class based on the safety function, and three other safety classes based on three technical fields: mechanical, electrical and automation. The structural safety class is included in the mechanical safety class. Structures in Loviisa NPP are generally not safety classified. The plant was built when the YVL-guides did not require classification of the structures and adopting new YVL-guide requirements has not yet required the classification of the structures. [30]

For example, a motor operated valve consists of mechanical parts and the actuator that is operated electrically and controlled with automation systems. A valve can then be classified to SC3 based on its mechanical parts, but to SC2 based on the electrical parts. The mechanical class can also be higher than the other classes due to there being structural requirements for the structure of the piping section, but the valve itself is not required for important safety functions. The electrical safety class of a consumer of electricity covers the component and the whole electricity supply chain [20].

There are no exact numbers for the share of components categorized to each class in the power plant, but some approximate numbers can be obtained from LOMAX [29]. Valves

and their mechanical safety classes are used as an example to provide some insight on how the components are spread into different safety classes. Data from [29] was used to calculate the total number of valves and the total number of valves that are classified to each safety class according to YVL B.2 and then shares were calculated. The results are in Table 1 below:

Table 1 Safety classes and the share of total components that belong to the class. Data from [29]

Safety class	Share of total valves
1	0,64 %
2	5,26 %
3	15,86 %
EYT	78,25 %

.

3 Probabilistic Risk Analysis

In this chapter the PRA methodology is introduced with focus on nuclear PRA. The first section provides some background information related to PRA, also including definition of risk and historical overview of PRA. The second section shows how the PRA is divided into different levels. The third section introduces the concepts of component reliability and unreliability that are used in estimation of failure probability of a component. Then the contents of a PRA model and how the model is quantified are explained. Some special aspects of the Loviisa PRA model and results of the model are presented. In Loviisa NPP, the software used for creating and solving the PRA models is called RiskSpectrum and the data used in this thesis is calculated with version RiskSpectrum PSA 1.3.2 of the software. This and the following chapter therefore focus on PRA with basis of how RiskSpectrum functions.

3.1 Background

There are multiple definitions used for risk, but in this thesis the terminology related to risk and risk analysis is adopted from [31] where risk is defined as a set of scenarios each of which has a probability and a consequence. Risk analysis focuses on the hazards related to these scenarios and the following questions are considered [31]:

1. What can happen?
2. What is the probability of it happening?
3. What are the consequences if it happens?

PRA is a structured methodology used for identifying and analyzing risks in complex technological entities, such as NPPs, and for producing numerical estimates for risk metrics. In this thesis the term ‘Probabilistic Risk Analysis’ is used. Other terms used to refer to PRA include ‘Probabilistic Risk Assessment’ and ‘Probabilistic Safety Analysis/Assessment’. PRA is used to examine frequencies and consequences of accidents in NPPs by analyzing accident sequences and operation of the safety systems. [31] An accident sequence is defined as a series of events that begins from an initiating event (IE) that challenges safety functions and can potentially lead to core damage and afterwards to release of radioactive materials from the plant [13].

In Finland it is required in [14] that a PRA analysis is submitted to STUK when applying for a construction license of a plant and when applying for an operating license [14]. STUK defines more specific requirements for PRA models and their use in [24]. The main objectives for PRA in Loviisa NPP are according to [32]:

1. Estimation of CDF and LRF
2. Identification of accident sequences, systems, components and functions that are most important with respect to risk
3. Identification of possible requirements for plant modifications
4. Estimation of probability for containment bypass in core damage events
5. Education of operation and maintenance personnel about risk significant aspects, prevention of them and the mitigation of their consequences

The PRA methods for NPPs were first used in USA in Reactor Safety Study led by Norman Carl Rasmussen in the 1970s. The study was started in 1972 and the report Reactor Safety

Study WASH-1400 [33] was published in 1975. The objectives of the study were to evaluate the consequences of a serious accident in a large modern light water reactor and the probability of their occurrence and to compare the risks associated with nuclear power to other risks Americans were subject to. The staff of Reactor Safety Study consisted of about 40 scientists and engineers and cost 4 million USD in currency of the 1970s. The team managed to estimate that the frequency of core melt for a PWR was about 6E-5 per reactor year and for boiling water reactors about 3E-5 per reactor year. [34] Results of the comparison between nuclear accidents and other types of accidents are shown in Figure 5.

Prior to the Reactor Safety Study fault-tree methods were utilized in the American aerospace sector in the 1960s. The Boeing Company with Bell Laboratories pioneered the use of fault tree analysis in design of the Minuteman intercontinental ballistic missile launch system for the U.S. Air Force. In 1966 the fault tree analysis was used in design of the Boeing-747 commercial jet and also NASA started using the fault tree methods in 1967 following the fire on Apollo-1. However, prior to WASH-1400, event tree methods were not yet utilized. [34]

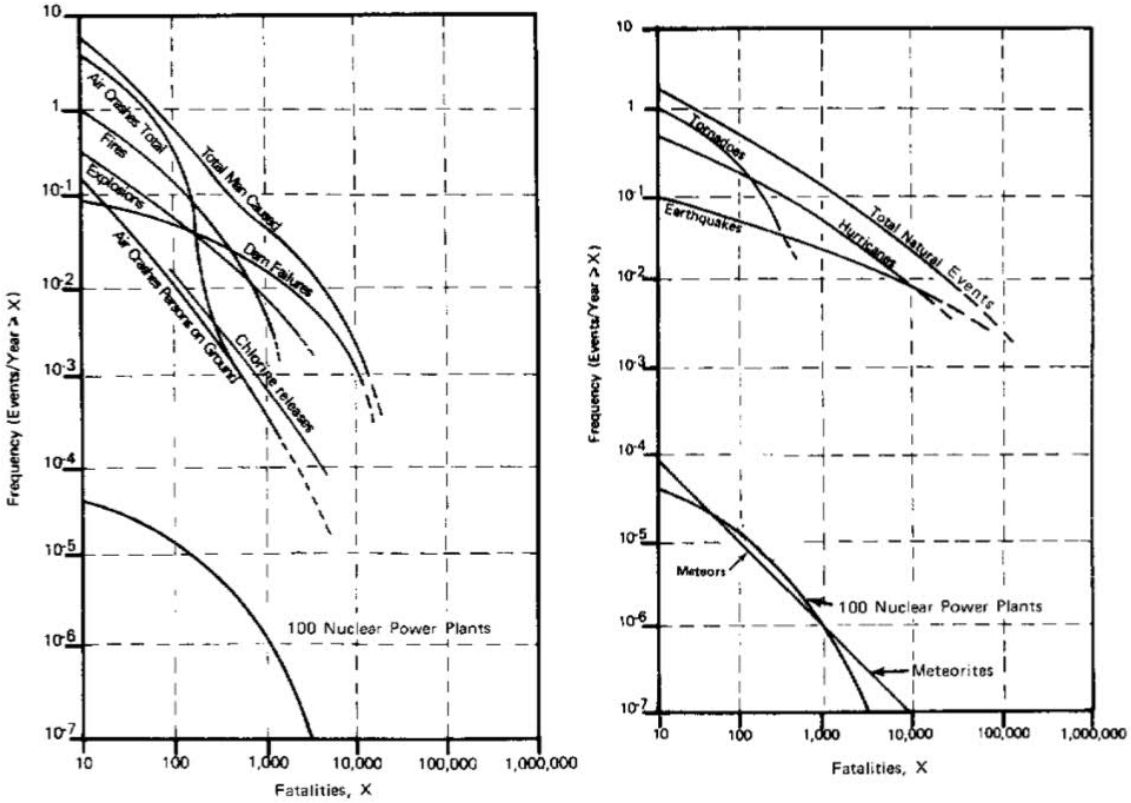


Figure 5 Results of WASH-1400. Risk of 100 operating NPPs is compared to accidents caused by man on the left and to natural accidents on the right. [33]

3.2 Levels of PRA

The three questions considered in risk analysis are answered to on three different levels of PRA. The three different levels of PRA were identified in PRA Procedures Guide [35]. The same levels of PRA are also identified in the Finnish legislation [24]. The three levels are called systems analysis, containment analysis and consequence analysis [35]. In addition to the different levels, PRA models are further divided based on operating modes.

Level 1: Systems analysis
Systems analysis constitutes a major partition of the PRA. The analysis on this level focuses on accident sequences that can lead to core damage. Objective is to identify all such accident sequences, their basic causes and the frequencies of their occurrence. The frequencies of accident sequences can then be used to determine the total CDF for the unit or plant. Identifying the sequences is achieved by first identifying all the events that challenge plant operation. Then the various responses, effects of external conditions and human errors are identified and analyzed. Results of level 1 PRA do not contain any notion on the consequences of the core damage. [35]

Level 2: Containment analysis
Containment analysis focuses on radioactive releases from the containment when core damage has occurred. Pathways and transportation of radionuclides from the damaged core into the environment of the reactor containment building are analyzed. A starting point for level 2 analysis is provided by level 1 results, including the CDF, accident sequences that lead to CDF and their frequencies. Level 2 analysis then focuses on the barriers and systems used for preventing the radioactive materials from leaving the containment building. The results include probability, time and mode of containment failure, and number of radionuclides released to the environment for each accident sequence. These results provide insight on the radiological consequences of each type of core damage and LRF can be calculated based on the results. [35]

Level 3: Consequence analysis
In consequence analysis the containment is assumed to have failed and the analysis on this level then focuses on the consequences of the radioactive releases. The consequences include health effects and impacts on environment and property. Health effects include both short-term injuries and long-term cancers. Environmental effects include contamination of the land area surrounding the plant. Consequences are typically expressed as early fatalities, latent cancer fatalities and property damage. Consequences analysis begins with estimating the spread of radioactive materials based on location of the release from the plant, surrounding terrain and weather conditions. This information, along with local population density information, can be used to estimate how many persons are exposed to the radioactive release. [35] According to [24] level 3 PRA is not necessary to be submitted to STUK in Finland and only level 1 and 2 PRAs are required.

Operating modes
NPPs operate in multiple different operational modes along the year, mainly due to scheduled annual outages. For the most part of the year, the plants operate at their nominal power. Operating mode influences operation of multiple systems at a specific time. Due to the operational differences, and differences in reactor criticality and other conditions, the PRA models need to be different for each operating mode. As a result, the analysis within level 1 and 2 PRA is further divided into analysis of each operating mode. The total CDF and LRF are both calculated as a sum of the CDF and LRF of each operating mode. There are six operating modes defined for Loviisa NPP and they are [36]:

1. Refueling shutdown
2. Cold shutdown
3. Hot shutdown
4. Hot standby

5. Startup
6. Power operation

The plant is taken through these modes in this order when it is started from shutdown, and in opposite order when it is being shut down. The operating modes are defined based on physical parameters (primary circuit temperature, boron concentration, reactor power), component states (control rod position, reactor cover position) and governmental regulations [36]. For the Loviisa PRA model the six modes are further divided into total of 18 different operating modes based on which components or subsystems are under maintenance and based on requirements set for safety systems [37]. While power operation covers about 90 % of a calendar year, the accident sequences occurring during power operation contribute to under 50 % of the total CDF for LO1.

3.3 Component reliability and availability

Component reliability and availability are essential subjects in PRA. Components can be either functioning or failed at a given time. The state of the component changes by time. All components will fail eventually and for non-repairable components this failed state is permanent. A repairable component is in the failed state for the duration from failure detection to failure repair. Change from functioning state to a failed state is called a failure and change from failed state to functioning is called a repair. In reliability engineering, the state of component after a repair is often considered "as good as new". [38] In this thesis a component being in functional state or available means that the component can perform a specified task. For example, a valve can close. This does not include any notation whether the valve is able to open. Component state, reliability and availability are considered to be specific to one failure mode of a component.

Reliability of a component is defined as probability that a component stays functional for a specified period of time t. Unreliability is the opposite of this. Unreliability measures the probability that a component has failed one or more times during the specified period of time t. Reliability and unreliability are used when non-repairable components are considered. Availability and unavailability are used for repairable components. Availability is defined as the probability that a component is functioning at a point in time t, given that the component was functioning at $t = 0$. Unavailability of a component $U_i(t)$ is the probability that the component is in failed state at a point in time t, given that the component was functioning at $t = 0$. [38]

Four classes of unavailability are identified for components in the PRA model for Loviisa NPP [39]:

- K: Unavailability due to critical failures that cause the component to be in failed state immediately after failure.
- L: Unavailability due to latent failures that do not cause the component to be in failed state immediately after failure, but the repair of the failure makes the component unavailable. Failure needs to be fixed before it evolves into a critical failure.
- M: Unavailability caused by scheduled maintenances, periodic tests or other scheduled non-failure related activities that cause the component to be unavailable
- H: Unavailability due to human errors during scheduled maintenances, periodic tests or calibrations

Only unavailability of class K and L are considered relevant when considering safety classification in this thesis because only they are related to component failures. Calculation of unavailability for failures depends on how a component is operated and three different classes are identified for this purpose. Class A components are in standby and are not operated unless they are required. Failures of standby components are noticed only when the component is used either in periodic tests or on demand. Class B components are in continuous operation and their failures are detected immediately. Class C components are in alternating operation. [39] An example of alternating operation is two pumps out of which one is in standby for four weeks while the other one is operating for those four weeks. The pumps switch from operating to standby and vice versa every four weeks.

Unavailability is calculated as a function of failure rate λ_i and the average time the component is unavailable after each failure. This time includes time from failure detection to component restoration τ_i and the time the component is in failed state prior to detection. The latter is usually calculated based on time interval between periodic test runs T_i. The failure data can be obtained as generic data or plant data. Generic data is data collected from literature sources that use data from multiple power plants. Issues with generic data are that the components are in different plants under different conditions and different maintenance programs and the manufacturers can also be different. When the databases for generic data are collected, the detection methods of failures are not specified. Plant data is plant specific data and therefore more accurate for the plant and components that are being analyzed. There can be too little operational experience for some components, or the failures are so rare that plant data cannot be used, and generic data needs to be used instead. [39] Next, the calculation of unavailability is explained as it is calculated for components in the Loviisa PRA model [39].

Unavailability for standby components is calculated based on generic data as

$$U_i = \lambda_i \left(\tau + T_o + \frac{T_i}{2} \right) \tag{1}$$

where T_o is time for which the component is required to function after an IE. Value for this is usually 24 hours. $\frac{T_i}{2}$ is a half of the time interval between test runs. Failures of standby components are not detected immediately. The unknown amount of time between failure and failure detection would average to $\frac{T_i}{2}$ in an infinitely large sample. For components in alternating operation the time interval between operating periods is used. For components in constant operation $T_i = 0$ and unavailability can be calculated as

$$U_i = \lambda_i (\tau_i + T_{o,i}) \tag{2}$$

Use of equation (2) assumes that all failures are detected in the periodic tests. When plant data is used instead, the unavailability is divided into three parts depending on how the failures are detected:

$$U_i = U_{i,KS} + U_{i,KM} + U_{i,KD} \tag{3}$$

where $U_{i,KS}$ is unavailability due to failures detected in a periodic test or scheduled maintenance, $U_{i,KM}$ is unavailability due to failures detected immediately and $U_{i,KD}$ is

unavailability due to failures detected on demand. The method of failure detection affects how much of the interval between periodic tests needs to be taken into account for calculating the unavailability.

The unavailability due to failures detected in periodic tests is

$$U_{i,KS} = 1 - \frac{1 - e^{-\lambda_{KS} T_{KS}}}{\lambda_{KS} T_{KS}} \times \frac{\mu_{KS}}{\lambda_{KS} + \mu_{KS}} \quad (4)$$

Where μ is restoration rate $\mu = \frac{1}{\tau}$. Unavailability due to failures detected by other methods are calculated similarly, but $T_{KM} = 0$ and $T_{KD} = 0{,}5\ T_{KS}$. For immediately detected failures then applies

$$U_{i,KM} = \frac{\lambda}{\mu + \lambda} \quad (5)$$

3.4 Contents and quantification of a PRA model

In this section the contents of a PRA model and quantification of the PRA model are introduced. The contents include BEs, IEs, fault trees and event trees.

3.4.1 Initiating and basic events

BEs and IEs are both events on the highest resolution of a PRA model. The occurrence of other larger events modelled in the model are determined based on occurrence of BEs and IEs while the BEs and IEs are not broken further into more detailed events. IEs are events that disrupt steady operation of the plant. They trigger accident sequences and require activation of plant control and safety systems in order to prevent core damage from occurring. [13] The amount of IEs and the scope of IE identification partly define the scope and accuracy of the PRA model because the amount of accident sequences is relative to the amount of IEs [39]. Grouping of IEs is then also necessary to reduce the amount of possible accident sequences. The grouping of IEs is based on the threats the IEs pose to the reactor core integrity and the safety functions that the mitigation of accidents requires. IEs that pose similar threats and require the same safety functions are grouped in the same group. [40]

IEs can be either from internal or external sources. Internal IEs can be caused as a result of a failure of an SSC, leakages, erroneous operation or fires. [39] For example, a low primary coolant flow can be defined as an IE. If the flow is reduced enough, reduction of heat transfer from the reactor core could lead to core damage. To prevent this, another system must be operated to remove the heat from the core. [40] External IEs are events caused by conditions that are external to the plant. These conditions include abnormal weather conditions, earthquakes and high water level. [39]

BEs are events that do not initiate an accident sequence, but their occurrence has an effect on whether the IE propagates into core damage The BEs can also be divided into internal and external BEs. Internal BEs include human errors, maintenances and technical failures of components. The technical failures of components include all their relevant failure modes. External events include events external to the plant. [40]

Events are considered to be binary variables in PRA models. Binary variables can have two different values, the event either occurs or does not occur. In addition to events, also sets and clauses are considered to be binary variables. [41] For BEs, these two possible states are defined as

- $X_i = 1$ means that the BE occurs, for example a component is unavailable
- $X_i = 0$ means that the BE does not occur, for example a component is available

The values are defined similarly for IEs that are represented with symbol Y_j. However, the occurrence of these events is measured with different parameters. The parameter used for IEs is their frequency $f_j = \mathrm{Fr}(Y_j = 1)$ in unit $\frac{1}{a}$ and it can have values in range [0,∞). For BEs, BE probability $Q_i = \Pr(X_i = 1)$ is used. This probability can have values in range [0,1]. When considering component failures, or other events leading to component unavailability, the BE probability is often determined with the unavailability.

$$Q_i = U_i \tag{6}$$

The occurrence of BEs is considered to be mutually independent, meaning that occurrence of one BE has no impact on the occurrence of another BE. IEs are all considered to be mutually exclusive, meaning that if one IE occurs, another will not occur at the same time. It is also possible to set a group of BEs mutually exclusive in RiskSpectrum. [42] For example, the different failure modes of a component modelled with separate BEs could be considered mutually exclusive, but no BEs have been set mutually exclusive in Loviisa PRA model.

3.4.2 Common Cause Failures

There can be intercomponent and intersystem dependencies between components which cause the failure of one component to affect the failure probability of another. Loss of an electrical system can impact the components that get their power from the electrical system or an automation failure affects the functioning of another system. These dependencies are taken into account when constructing fault and event trees. [40]

There are also common cause failures (CCFs). A CCF is an event in which two or more components are in failed state due to a single shared cause and the failures of the components do not happen independently of each other [41]. CCFs defeat the benefit of redundancy. Some of the potential causes for CCFs include internal conditions, such as high temperature or humidity, human errors, such as failed calibration of multiple sensors, and external events, such as earthquakes or fires. [40] Defence against CCFs can be provided by utilizing the diversity principle, staggered testing, staggered maintenance or physical barriers [41].

CCFs are modelled in the fault trees with BEs that are separate from individual failure events. Their probabilities can be determined with parametrical models or based on operating experience. The data on some CCFs is scarce and experiences from multiple plants may need to be used. It is assumed in the parametrical models that ratios between rates of independent failures and CCFs are more universal than the failure rates of independent failures. [39] Parametric models include beta-factor model, multiple Greek letter model and alpha-factor model. Parametric models can be applied for CCF groups. A CCF group is a group of components that can be affected by the same CCF. [42]

Beta-factor model is the simplest model of these three and it is described next based on [41]. In this model a factor is used that represents the ratio of CCF failure rate to independent failure rate of a component. The total failure rate of a component is

$$\lambda_{tot} = \lambda_I + \lambda_c \tag{7}$$

where λ_{tot} is the total failure rate of the component, λ_I is the failure rate due to individual failures of component and λ_c is the failure rate of the CCFs. The beta-factor is then defined as a ratio of CCF failure rate to total failure rate and it can be interpreted as the probability a component fails due to a common cause given that it fails.

$$\beta = \frac{\lambda_c}{\lambda_{tot}} = \frac{\lambda_c}{\lambda_c + \lambda_I} \tag{8}$$

In the beta-factor model the failure rate is defined for events in which all the components in the CCF group fail. The other models include more parameters which allow to define factors for failures of only k out of the m components in a CCF group. [41]

3.4.3 Event trees

Event and fault trees are both graphical expressions of Boolean algebra. Boolean algebra is a branch of algebra that is applied for binary variables, such as the events, sets and clauses mentioned earlier. [41] An event tree is a representation of multiple accident sequences that originate from an IE and consist of same plant responses to the IE that have an impact on the consequence. There are two types of event trees: system event trees and containment event trees. System event trees are used on level 1 PRA and containment event trees are used on level 2 PRA. [35]

An event tree visualizes how the progression of an accident sequence depends on failures and successes of safety functions, barriers or other measures designed to prevent the propagation of the IE. [40] By using the glossary used in RiskSpectrum, these successes and failures are called function events and the possible end states of the plant are called sequence top events. The probabilities of function events are defined with either fault trees or based on a BE. [42] A sketch of an event tree is shown in Figure 6 where all the function events represent safety functions. In actual models, the safety functions are often not identified this clearly. The leftmost event of the event tree is the IE. Then, the IE is followed by multiple function events. The order of function events in event trees follow a chronological order or other logical order that follows the interdependence between the events and the order in which the preventive actions are required [40].

A path that represents a sequence begins from the IE and branches into two branches based on the occurrence of the function events. The upper branch represents a success of a safety function and the lower branch represents a failure of the safety function. The excess branches that do not have an impact on the outcome of the accident sequence, or are logically impossible, are pruned off. At the end of each sequence the sequence is identified with a unique ID and its consequence, the sequence top event, is defined. On level 1 the consequence is commonly either OK state of the plant or core damage. On level 2, the consequence is the amount and time of radionuclide release.

A Boolean expression can be solved for the sequence top events from an event tree. There are three basic operators used in Boolean algebra for events and they are denoted as follows: [41]

Events A and B happen (intersection) $A \cdot B$
Event A or B happens (union) $A + B$
Event A does not happen (negation) $-A$ or $\bar{A}$

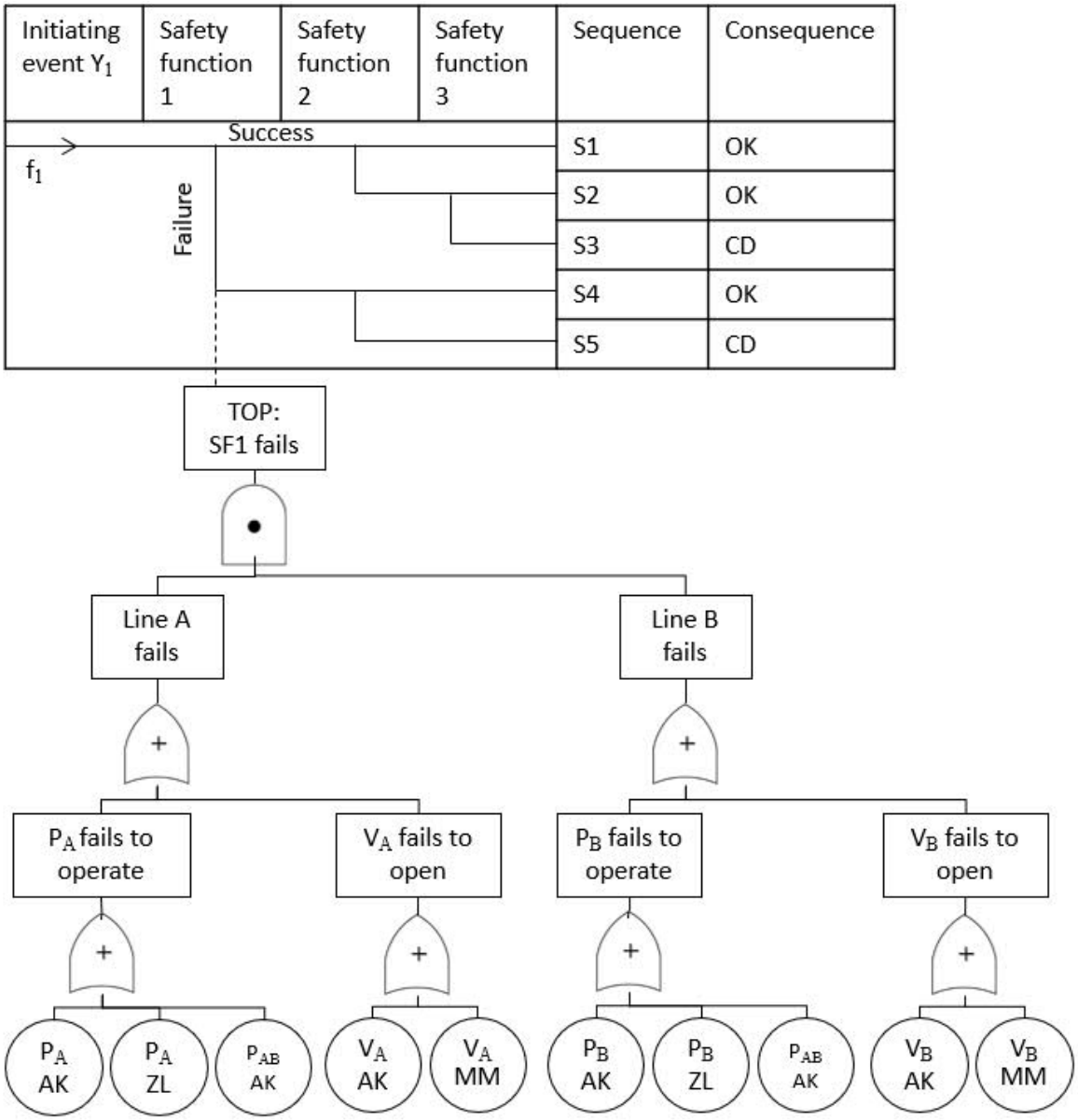


Figure 6 A sketch of an event tree for IE Y_j and a fault tree for the failure of safety function 1. The event tree is pruned of impossible or unnecessary branches. All the other safety functions would also have a fault tree connected to them. The safety function consists of two redundant identical pumping lines that both consist of a valve (V) and a pump (P). The fault tree top event is failure of safety function 1. Pump A can be unavailable due to critical failure to open (P_AAK), a latent failure (P_AZL), or due to a CCF of both pumps ($P_{AB}AK$).

In Figure 6, core damage is defined as the sequence top event for sequences S_3 and S_5. Occurrence of both sequences can be defined based on the IE, and the safety functions. E_1 represents the failure of safety function 1 and $\bar{E}_1$ the success of the safety function. The core damage due to events in this event tree can then be expressed as:

$$CD = S_3 + S_5 = Y_1 \cdot \bar{E}_1 \cdot E_2 \cdot E_3 + Y_1 \cdot E_1 \cdot E_2 \quad (9)$$

3.4.4 Fault trees

Fault trees are used to develop a deterministic description on how an undesirable event, such as the failure of a safety function depends on the occurrence of BEs. The undesirable event is represented with an event called fault tree top event. [40] A Boolean expression for the occurrence of the top event can be solved from the fault tree and the top event can be expressed as [43]

$$T = \phi(\boldsymbol{X}) = \phi(X_1, X_2, \dots X_n) \quad (10)$$

where T is the top event, $\phi()$ is called the structure function of the system, $\boldsymbol{X}$ is a vector consisting of all the BEs in the fault tree, X_i is a BE and n is the number of BEs in the fault tree. The FT top event can then have two values: [43]

- $T = \phi(\boldsymbol{X}) = 1$, the top event occurs, i.e. the system fails
- $T = \phi(\boldsymbol{X}) = 0$, the top event does not occur, i.e. the system does not fail

Fault trees follow a 'backwards logic'. The analysis begins from the FT top event. First, all the intermediate events that can cause the FT top event are identified. Intermediate events are caused by combinations of other events further down in the fault tree. The intermediate events are analyzed and divided further into smaller intermediate events. This is continued until the root causes, the BEs, for which probabilities can be estimated are identified. [31]

In a fault tree, the Boolean operators are represented with logical gates between events. The different types of events are also expressed with their own symbols [31]. The most commonly used symbols for events and gates are presented in Table 2. A sketch of a fault tree is illustrated in Figure 6 below the event tree and the same symbols are used in the sketch.

The fault tree in Figure 6 expresses the failure of safety function 1 as a function of occurrence of BEs. Failure of the function is the FT top event. This event is divided into two intermediate failures, both of which are failures of redundant pumping lines. If both lines fail, the safety function also fails. Therefore, the pumping lines are considered to be parallel with respect to reliability analysis. The intermediate events are further divided into smaller intermediate events, the failure of a valve and a failure of a pump. Failure of either one of them is only required for the line failure. Therefore, the pump and valve are considered to be in series. Then, these failures of a component are divided further into different failure modes that are represented by the BEs.

A system is called a coherent system if failures of subsystems or components do not improve the system. Using the structure function, coherency of a system requires that that all of the BEs are relevant, i.e. they contribute to the system state: [43]

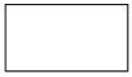
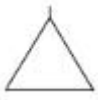
$$\phi(\boldsymbol{X}, X_i = 1) \neq \phi(\boldsymbol{X}, X_i = 0) \quad (11)$$

for some X_i. In addition, it is required that the structure function is monotonically increasing: [43]

$$\phi(\boldsymbol{X}, X_i = 1) \geq \phi(\boldsymbol{X}, X_i = 0) \quad (12)$$

for all X_i. When considering a fault tree, fulfillment of these two requirements requires that it is constructed of AND and OR -gates. [43] If there are BEs that are considered mutually exclusive, exclusive-or gates, or NO-gates in the fault tree, the fault tree will be non-coherent. If the failure modes of a component were considered mutually exclusive, the occurrence of the one with worse consequences would be prevented by the occurrence of the one with better consequences. The occurrence of an event would therefore decrease the risk.

Table 2 Common event and gate symbols for fault trees. Symbols and definitions from [31].

Events	
Symbol	Description
	BE. An event that requires no further division into smaller event.
	Intermediate event. An event that occurs because of one or more predecessor events connected to the intermediate event with logic gates.
Gates	
Symbol	Description
	AND -gate. Output of the gate occurs if all the input events occur. Redundant subsystems or components commonly require the failure of both, and they are connected with an AND-gate.
	OR -gate. Output of the gate occurs if any of the input events occur. Components that are in series, i.e. failure of one component fails the subsystem, are connected commonly with an OR-gate.
	Transfer in from another fault tree. The fault tree is located elsewhere, and this enables linking another event tree to a gate

3.4.5 Quantification

Event and fault trees are both deterministic descriptions of how the sequence and FT top events can happen. In order to get numerical results from the PRA model, a Boolean expression for the sequence top event needs to be solved from event and fault trees first. Then the Boolean expression can be quantified by using the values calculated for BE and IE

parameters. There can be multiple dependencies between safety functions through shared equipment, or due to CCFs. A method for solving the Boolean expression is called fault tree linking and it is described in [35] and also used in RiskSpectrum. In this method, the Boolean expression for the sequence top event is solved by converting event trees into fault trees and then linking multiple fault trees together. The large resulting fault tree is called a sequence fault tree in RiskSpectrum [42]. Sequence fault trees, unlike system fault trees, do include IEs.

When event trees are converted to fault trees, fault tree top events are created for the sequence top events of interest. Then, intermediate events are created for all the accident sequences that can lead to the top event. The intermediate events are connected to the top event with an OR-gate. The IE and function events that occur in an accident sequence are connected to the intermediate events representing accident sequences with an AND-gate. The fault trees of related safety functions are connected to these intermediate events. [35] Conversion of the event tree in Figure 6 to a fault tree, whose top event is core damage, is demonstrated in Figure 7.

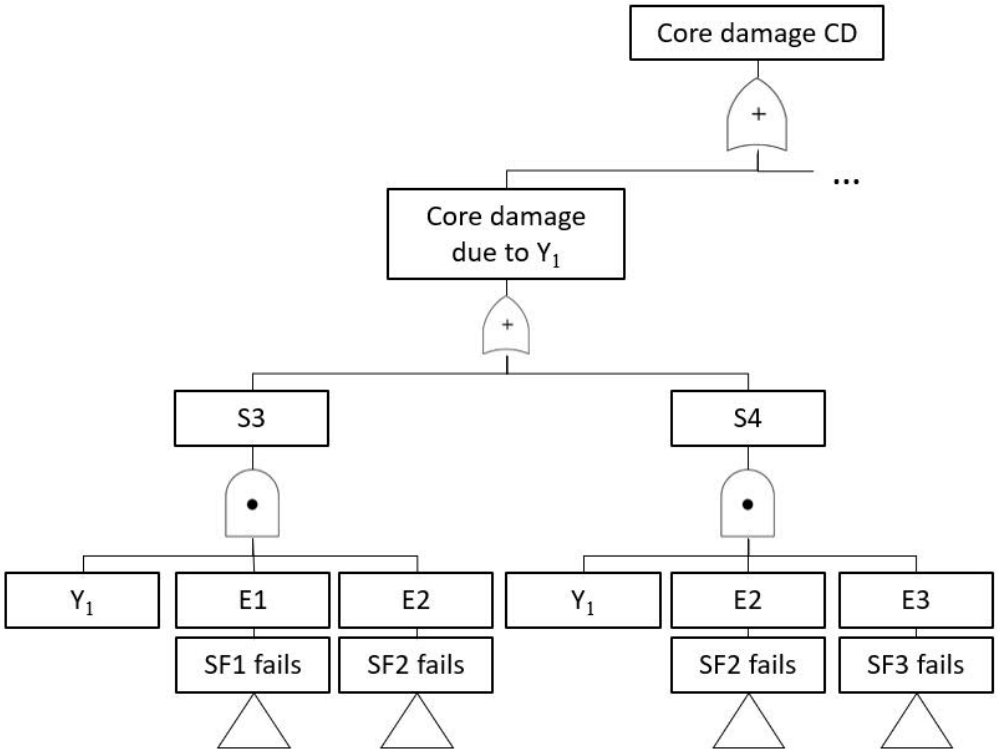


Figure 7 Event tree from Figure 6 converted into a fault tree with core damage as the sequence top event

The Boolean expression for FT top event of a fault tree can be solved by solving minimum cut sets (MCSs). A cut set is a set of BEs and IEs whose occurrence ensures that the top event also occurs. An MCS is a cut set from which any of the events cannot be removed without the set losing its status as cut set. [31] MCSs define all the possible combinations of BEs and IEs that can cause the top event to occur. A top event occurs if and only if at least one MCS occurs. Occurrence of the FT top event can then be defined based on the MCSs:

$$TOP = M_1 + M_2 + \cdots + M_m \tag{13}$$

Where TOP is the top event, and M is an MCS and m is the total number of MCSs solved from the fault tree. MCSs can be solved for any fault trees, but when they are solved for sequence fault trees, they include one IE and one or more BEs. The occurrence of one MCS is measured with its frequency. The Boolean expression for a single MCS is

$$M_l = Y_j \cdot X_1 \cdot X_2 \cdot \ldots \cdot X_n \tag{14}$$

And the frequency of the occurrence of this MCS is

$$\mathrm{Fr}(M_l) = f_j \prod_{i=1}^{n} Q_i = f_j Q_1 Q_2 \ldots Q_n \tag{15}$$

RiskSpectrum calculates the MCS frequencies generally at the same time as the MCSs are solved in order to ignore the very rare and insignificant MCSs. When the frequency undercuts a limit called cutoff limit, the MCS is not solved further in order to reduce computation time and memory requirements. [42] The cut-off limit used for quantification of Loviisa PRA model on level 1 PRA was $2 \times 10^{-15}\,\frac{1}{a}$ in 2019 [39] and the total number of MCSs for power operating mode is over two million.

One approach for solving MCSs from a fault-tree is called the top-down approach. The approach begins from the top event that is first solved on basis of the intermediate events highest in the tree. Then the intermediate events are further solved based on other events, until there are only BEs left in the equation. When there is an AND-gate, both events below the gate are added to the cut set and when there is an OR-gate, the cut set is duplicated to match the number of events under the OR-gate. [42]

The MCSs are grouped into groups that are mutually exclusive for calculation of the total top event frequency. MCSs can be considered mutually exclusive if they include a different IE or they include mutually exclusive BEs. Multiple MCSs that do not share mutually exclusive events can occur at the same time due to the independency of BEs. Therefore, the accurate calculation of the probability that the IE shared by a group of MCSs leads to the top event needs to be calculated based in inclusion-exclusion principle. [42] This principle is explained in more detail in [31].

The number of MCSs in a single PRA model is very large and therefore approximations are used. One of the first order approximations is called rare event approximation and use of the approximation assumes that the probability of two MCSs occurring at the same time is insignificant. [31] The difference between how the uses of inclusion-exclusion principle and rare event approximation assume the occurrence of three mutually independent MCSs is illustrated in Figure 8. The total top event frequency according to rare event approximation is calculated according to [31] as:

$$f_{TOP} = \sum_{l=1}^{m} \mathrm{Fr}(M_l) = \mathrm{Fr}(M_1) + \mathrm{Fr}(M_2) + \cdots + \mathrm{Fr}(M_m) \tag{16}$$

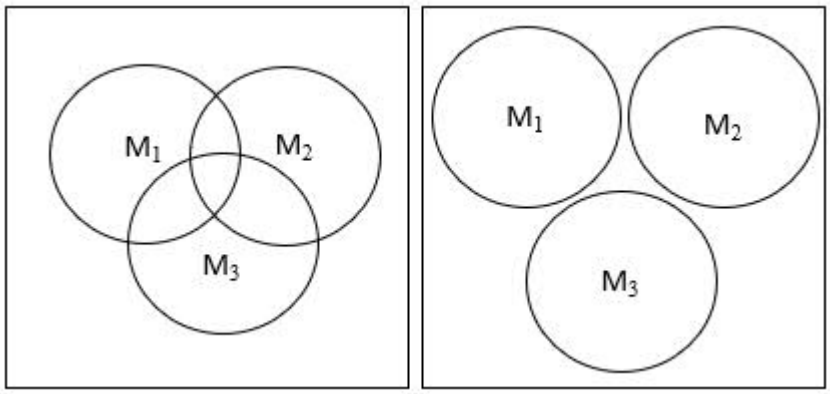


Figure 8 Occurrence of three mutually independent MCSs illustrated on a Venn-diagram based on inclusion-exclusion principle (left) and on rare-event approximation (right)

The approximation used by default in RiskSpectrum is called MCS upper bound method which is considered more accurate than the rare event approximation but is not as accurate as inclusion-exclusion principle. In this method the probability of a single MCS occurring given that the IE occurs are used to calculate the total probability that the top event occurs given that the IE occurs. Probability an MCS occurs given that the IE occurs is the product of the probabilities of BEs in the MCS:

$$\Pr(M_l|Y_j) = \prod_{i \in l} Q_i \tag{17}$$

The total probability of top event given occurrence of the IE occurs is then calculated as

$$\Pr(TOP|Y_j) = 1 - \prod_{l=1}^{n} (1 - \Pr(M_l|Y_j)) \tag{18}$$

where n is the total number of MCSs in the set. Multiplying this probability with the IE frequency yields the total top event frequency contributed by this set of MCSs. The total top event frequency is then the sum of the frequencies contributed by each set:

$$f_{TOP} = \sum_{j=1}^{m} f_j \Pr(TOP|Y_j) \tag{19}$$

Where f_{TOP} is the total top event frequency, f_j is the IE frequency and m is the total number of IEs. Both the rare event approximation and the MCS upper bound method are considered conservative, meaning that they overestimate the sequence top event frequency. [42]

3.5 PRA model of Loviisa NPP

The PRA model of Loviisa NPP is a living PRA model, meaning that it is updated annually to match the current operational experiences and plant data. Failure data for components is collected from work orders and the failure rates are recalculated annually. The model is also updated when new plant upgrades are changed, or new significant risks are identified. The

main report for the PRA is updated annually after annual outages. The report is also delivered to STUK each year. [32]

Figure 9 shows how the CDF and risk distribution has changed between years 1996 and 2018. The total CDF has not yet reached the $10^{-5}\frac{1}{a}$ limit that is required from new plants, but the CDF is very close to that value. Changes that increase the CDF have generally been changes to the model, e.g. inclusion of weather effects during shutdown modes. The CDF has also been decreased significantly due to changes made to the plant unit.

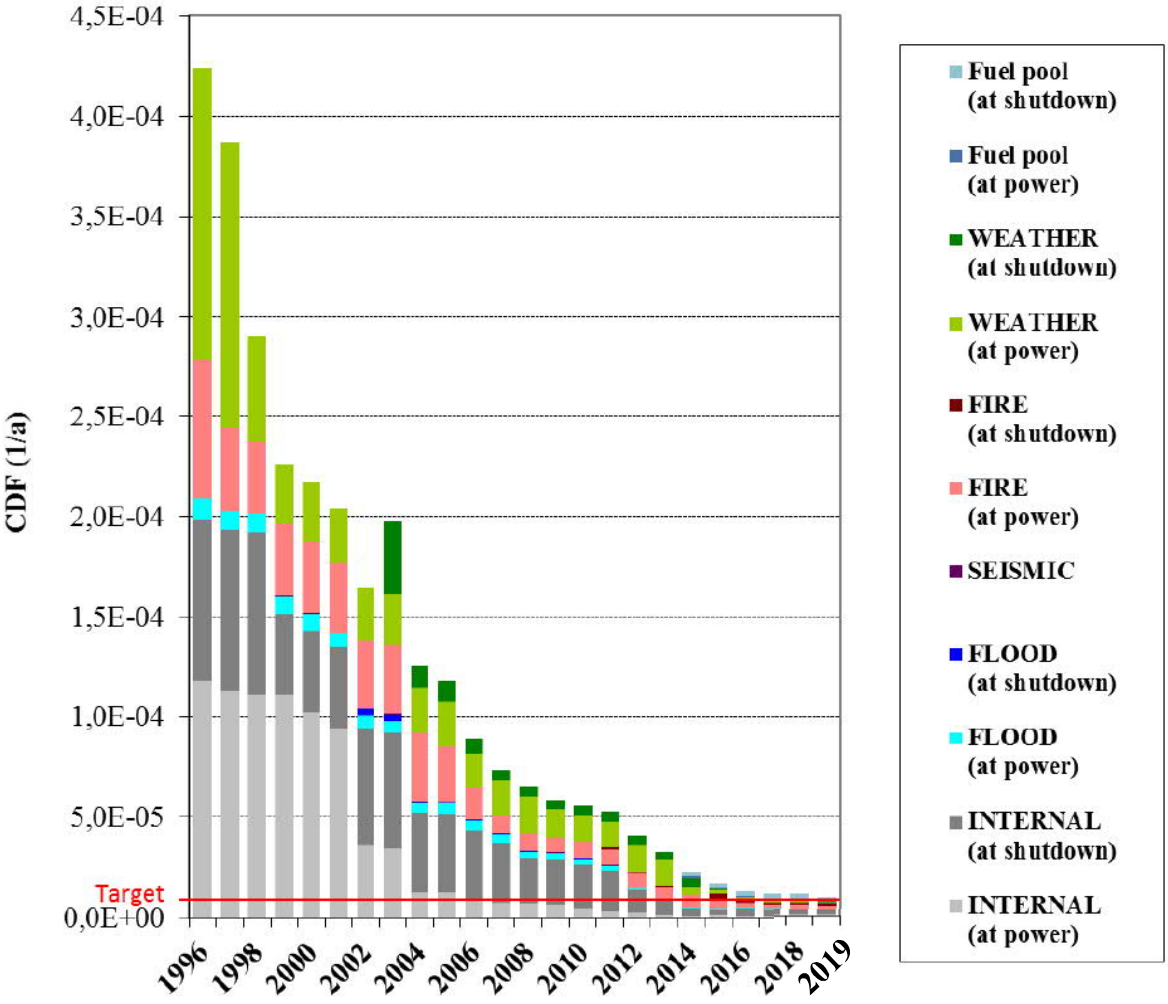


Figure 9 Progression of Loviisa NPP CDF and risk distribution. Red line marks the target value for CDF of new plants $CDF = 10^{-5}\frac{1}{a}$ [39]

The PRA model is constructed as based on large fault trees and small event trees principle. The event trees are partly integrated to a large fault tree, Figure 10 shows how an event tree is represented in the model. This example is for core damage due to a large LOCA in the power operating mode. The IE, and a fault tree for the conditional probability of the IE leading to core damage are all connected to an AND-gate. This structure itself is connected with an OR-gate to an intermediate event that represents all the internal initiators during power operation. Figure 11 then shows how the conditional probability is formed from different types of failures of functions. This kind of integration of event trees into a large

fault tree should not have any impact on the solving of MCSs and should not have effect on the results.

The BE probabilities and IE frequencies are calculated outside of RiskSpectrum even though RiskSpectrum offers the ability to input event parameters and calculate the probabilities within the application. The BEs and their probabilities are collected to an excel-sheet called PSADATA [44]. In the 2019 model revision the number of BEs modelling LO1 components was around 7600 and the number for LO2 unit was around 7200. IEs are collected to excel-sheet T15X2 [45]. The total number of IEs was around 600. The probabilities or frequencies are determined for all the events and for all operating modes of the plant [39].

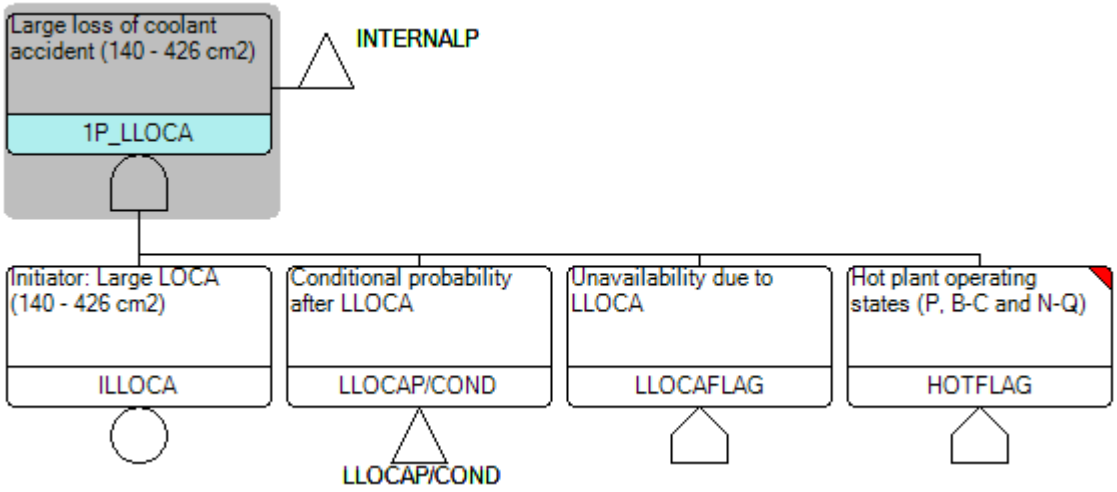


Figure 10 An event tree of a large LOCA integrated to the large fault tree

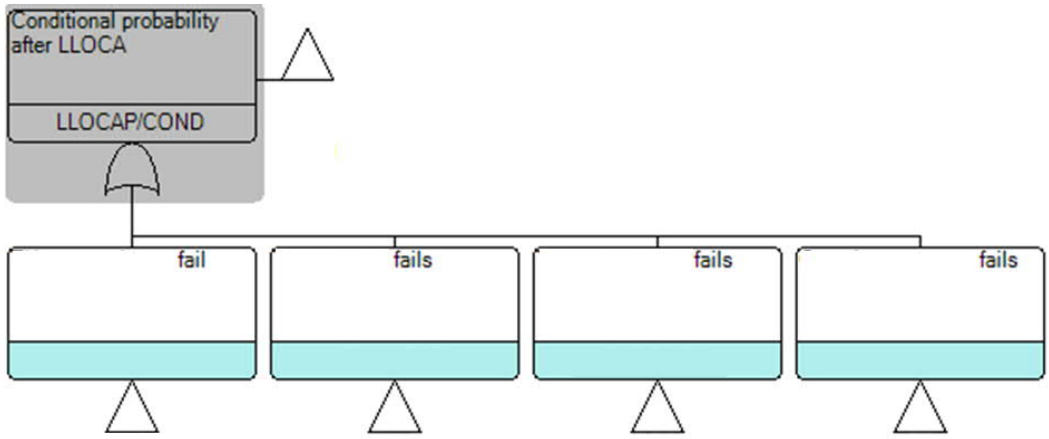


Figure 11 Conditional probability of large LOCA leading to core damage (the intermediate events are censored)

4 Risk Importance Measures

One of the main objectives of a PRA is to identify the SSCs most important to safety. RIMs are one of the measures that can be used for this objective. RIMs are calculated for the BEs and IEs and are used in multiple applications. There are three main categories for application of RIMs identified in [46]:

1. Optimization of plant design by adding or removing SSCs
2. Optimization of plant performance by adjusting test and maintenance strategies
3. Evaluating the effects of daily changes to configuration

A fourth category, uncertainty analysis, was also included in [40]. Concrete applications of RIMs include risk-informed in-service inspections (RIISI) of piping sections and components, risk-informed allowed outage time optimizations and risk-informed preventive maintenance.

There are multiple RIMs that are commonly discussed in literature and can be calculated by RiskSpectrum or are calculable from the RiskSpectrum results. These RIMs measure the importance of an event from multiple different perspectives and have different kinds of uses. This chapter will first introduce the definitions and calculation of these RIMs for BEs and IEs, and the different interpretations of the values. Then, the application of RIMs to measure SSC importance on different levels of SSC hierarchy is discussed. Next the RIMs to be used in the comparison chapter are selected. Then, the effects that the safety class of a component can have on the RIM values of the events modelling the component are discussed. In the last section, a foreign application of RIMs in safety categorization of SSCs is introduced.

4.1 Calculation of risk importance measures

RIMs can be used to define the importance of any BE or IE, but the objective of this thesis only requires applying RIMs for the events used to model SSCs. Events such as weather-related events are ignored. And since in nuclear PRA the risk is measured with CDF and LRF, the RIMs are used to measure their impact on the CDF or LRF. The interpretations of RIM values are then also discussed based on nuclear PRA and its risk metrics. The RIMs are calculated and interpreted slightly differently for BEs and IEs and therefore the RIMs for BEs are described first, and then the differences of IE RIMs are described.

4.1.1 Importance measures for basic events

As mentioned in Chapter 3, the PRA model is different for different operating modes. Therefore, the RIMs are calculated for each operating mode separately. Then RIMs measuring the importance of an event across all operating modes can be calculated from the operating mode specific RIMs. Some expressions will be used when describing the calculation of different RIMs in this section:

- $f_{TOP,p}$ refers to sequence top event frequency in operational mode p. Unit for $f_{TOP,p}$ is $\frac{1}{year}$.
- f_{TOP} is the sequence top event frequency including all operating modes
- $f_{TOP,p}(Q_{ip} = 1)$ is the increased top event frequency when the probability of BE X_i is set to its maximum value, that is 1. Probabilities of all the other events including other failure modes of the component are set to their base values.

- $f_{TOP,p}(Q_{ip} = 0)$ is the decreased top event frequency when the probability of BE X_j is set to its minimum value, that is 0. All the probabilities of other events including other failure modes of the same component have their base values
- $f_{TOP,p}(\text{base})$ is the base top event frequency when all BE probabilities are at their base values
- $Q_{ip}(\text{base})$ is the base probability of X_i in operational mode p

RiskSpectrum calculates the adjusted $f_{TOP,p}$ values by adjusting the BE probability and quantifying the MCSs again. The MCSs are not solved again based on the new conditions and this results in some inaccuracies. A large share of MCSs that include a very rare event undercut the cutoff limit and they are not included in the calculations either when the probability is changed to unity. This results in an underestimation of the value of $f_{TOP,p}(Q_{ip} = 1)$. Therefore, for rare events the RIMs calculated based on $f_{TOP,p}(Q_{ip} = 1)$ are not always very accurate. Accurate calculations of this value would require that the whole model is solved again with the probability set to unity.

In addition to the previously mentioned expressions, a linear equation for risk is adopted from [46] and adjusted to express $f_{TOP,p}$ as a function of the BE probability. This equation is:

$$f_{TOP,p}(Q_{ip}) = a_{ip}Q_{ip} + b_{ip} \tag{20}$$

where

- $f_{TOP,p}(Q_{ip})$ is the top event frequency in operating mode p as a function of probability of X_i
- $a_{ip}Q_{ip}$ is the contribution of MCSs that include X_i to the total top event frequency
- a_{ip} is the slope of the equation
- Q_{ip} is the probability of X_i in operating mode p
- b_{ip} is the contribution of all MCSs that do not include X_i to the total top event frequency in operating mode p

A sketch plot for this equation is shown in Figure 12. This equation divides the top event frequency into two parts: frequency contributed by the MCSs that include X_i and the MCSs that do not include the event. Changing the BE probability changes the first part, but not the second. The equation is considered to be valid in [46] when all the BEs are independent and the model is coherent. The value of a_{ip} depends on the number of MCSs the event is included in, the number of events in the MCSs and the parameters describing the occurrence of the events. When considering components in an NPP, the value of a_{ip} depends on the location of the component in the plant, and the system structure around the component. For example, redundancy increases the number of events in the MCSs, and therefore decreases the value of a_{ip}. Q_{ip} depends on the component itself. These two factors, system structure and the unavailability of the component generally guide the importance of the component.

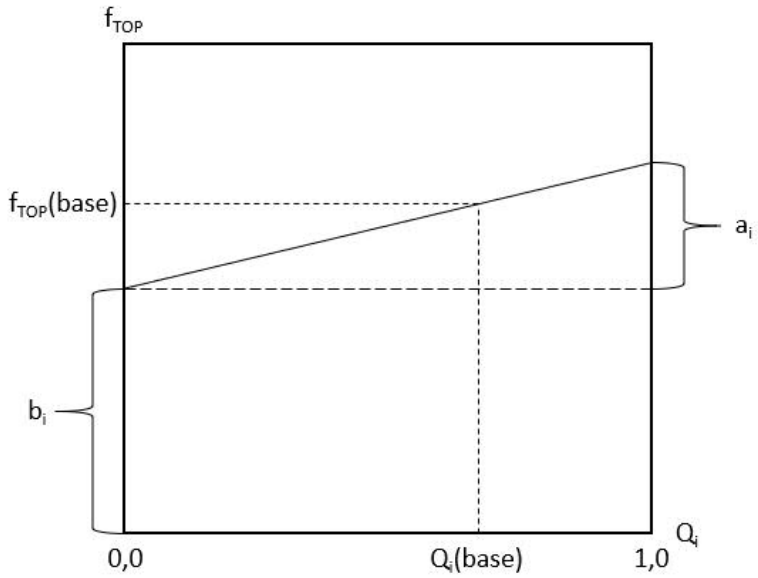


Figure 12 Plot of equation y. Drawn based on [46].

4.1.1.1 Fussell-Vesely

Fussell-Vesely importance measure (FV) of a BE is defined as the conditional probability that at least one of the MCSs that include X_i has occurred given that the sequence top event has occurred [47]. In [48] FV is also defined as the fraction of total risk contributed by MCSs that contain X_i. When total risk is measured with sequence top event frequency, FV can be calculated as:

$$I_{ip}^{FV} = \frac{\mathrm{Fr}(\bigcup_{i \in l} M_l)}{f_{TOP,p}(\mathrm{base})} \tag{21}$$

where $\mathrm{Fr}(\bigcup_{l|i \in l} M_l)$ is the total sequence top event frequency contributed by the MCSs that include X_i. Because FV is calculated as a ratio, the values are relative to the base top event frequency and it can have values in range [0,1]. Another method for calculating FV that is included in [46] is defined as follows:

$$I_{ip}^{FV} = \frac{f_{TOP,p}(\mathrm{base}) - f_{TOP,p}(Q_{ip} = 0)}{f_{TOP,p}(\mathrm{base})} \tag{22}$$

In the numerator, the frequency contributed by MCSs that do not include X_i is removed from the base frequency, leaving only the frequency contributed by the MCSs that do include X_i. This second method is also referred to as fractional contribution (FC) in [49] and criticality importance in [50]. RiskSpectrum can be used to calculate FV based on both of the methods [42] and both of the methods should produce very similar values in coherent PRA models according to [49]. Some deviations may still exist due to the use of MCS upper bound method instead of rare event approximation. Both methods of calculating FV can be expressed using symbols from equation (20) according to [46] as:

$$I_{ip}^{FV} = \frac{a_{ip}Q_{ip}(\text{base})}{a_{ip}Q_{ip}(\text{base}) + b_{ip}} \tag{23}$$

When $a_{ip}Q_{ip} \ll b_{ip}$, this is reduced to [46]

$$I_{ip}^{FV} \approx \frac{a}{b}Q_{ip} \tag{24}$$

The condition is true for most of the component related BEs in an NPP because the redundancy for the failure of a single component is high and it is very unlikely that a single failure mode of a single component contributes a large share of the total risk [46]. The value of FV therefore depends on the system structure and component unavailability. The values of FV are directly proportional to the unavailability.

It is described in [51] that FV can be used to show the relative reduction in risk when BE probability is reduced to zero and the relative increase in risk when the BE probability is doubled. Thus, FV can be used to define the maximum available relative decrease in risk by improving a component and to identify SSCs that provide the highest potential in reducing the risk by improving the availability of the SSC. After the improvement, the values of FV should drop and the SSC would not be seen as important anymore according to FV. [51] FV can also be used to identify SSCs that are the most likely to cause the sequence top event, and the repair of those SSCs is most likely to prevent the sequence top event. FV can therefore be utilized to prioritize inspection programs. [50]

When considering all plant operating modes, the FV value is calculated as a weighted average of operating mode specific FV values with the operating mode specific sequence top event frequency as the weighting factor [39]

$$I_i^{FV} = \frac{\sum_p \left(I_{ip}^{FV} f_{TOP,p}\right)}{\sum_p f_{TOP,p}} \tag{25}$$

Where the numerator is the total frequency contributed by the MCSs that include the BE across all operating modes and the denominator is the total top event frequency across all operating modes.

FV can also be used to solve all the other RIMs when the values of FV, BE probability and top event frequency are known. Solving the equation pair

$$\begin{cases} f_{TOP,p} = a_{ip}Q_{ip} + b_{ip} \\ I_{ip}^{FV} = \dfrac{a_{ip}Q_{ip}}{a_{ip}Q_{ip} + b_{ip}} \end{cases} \tag{26}$$

yields

$$\begin{cases} a_{ip} = \dfrac{I_{ip}^{FV} f_{TOP,p}}{Q_{ip}} \\ b_{ip} = \left(1 - I_{ip}^{FV}\right) f_{TOP,p} \end{cases} \tag{27}$$

Other RIMs also have this property, but RiskSpectrum rounds the RIM values to four significant digits. Other RIMs, such as Risk Reduction Worth (RRW), and Risk Achievement Worth (RAW), have their minimum value at 1. Therefore, all values below 1,0005 are all rounded down to 1,000. Use of such values to calculate FV, for example, would be counter-intuitive due to the loss of information.

4.1.1.2 Risk Reduction Worth

Risk Reduction importance measure (RR) shows how much the total risk would decrease if a BE would never happen [46]. When the BE is used to model a component failure, risk reduction shows the decrease in risk if the component was made perfect with respect to the failure mode. For example, a pump would never fail to start. RR shows the absolute decrease in top event frequency and it is calculated as [46]:

$$I_{ip}^{RR} = f_{TOP,p}(\text{base}) - f_{TOP,p}(Q_{ip} = 0) = a_{ip}Q_{ip} \tag{28}$$

It is more common to express risk reduction as a relative value. Then it is called RRW where the word "worth" refers to the worth of decreasing the unavailability by improving the component. [46] According to [40] the use of relative RIMs, like FV and RRW, has the advantage of being more robust than the absolute measures and therefore they are preferred over absolute measures [40]. Another term used to refer to RRW is risk decrease factor. RRW is calculated as [46]

$$I_{ip}^{RRW} = \frac{f_{TOP,p}(\text{base})}{f_{TOP,ip}(Q_{ip} = 0)} = \frac{a_{ip}}{b_{ip}}Q_{ip}(\text{base}) + 1 \tag{29}$$

RRW can have values in range [1,∞). The value of RRW shows the maximum available decrease in risk achievable by improving the component. [52] In addition, RRW can be expressed as a function of FV [46]

$$I_{ip}^{RRW} = \frac{1}{1 - I_{ip}^{FV}} \tag{30}$$

It can be seen from this relation that RRW and FV will give the same ranking for components. Both of the RIMs can be used to measure relative risk reduction, but FV is more commonly used for that purpose.

4.1.1.3 Risk Achievement Worth

Risk Achievement importance measure (RA) is similar to RR but RA measures the absolute increase in risk when a BE always occurs, i.e. the probability is 1 [46].

$$I_{ip}^{RA} = f_{TOP,p}(Q_{ip} = 1) - f_{TOP,p}(\text{base}) = (1 - Q_{ip})a_{ip} \tag{31}$$

It is assumed in this equation that the component is always in failed state with respect to the failure mode modelled with X_i, but the value can also be interpreted as the momentary increase in risk due to a failure. Risk achievement is also more commonly used as a relative importance measure called RAW. The term 'worth' now refers to the worth of maintaining the BE probability at its current value [52]. Another term used to refer to RAW in [53] is

risk increase factor that refers to the factor by which the risk increases due to failure of a component. RAW is calculated as a ratio between increased risk and base risk similarly to RRW [46] as

$$I_{ip}^{RAW} = \frac{f_{TOP,p}(Q_{ip} = 1)}{f_{TOP,p}(\text{base})} = \frac{a_{ip} + b_{ip}}{a_{ip}Q_{ip}(\text{base}) + b_{ip}} \tag{32}$$

Like RRW, RAW can have values in range [1,∞). When $a_{ip}Q_{ip} \ll b_{ip}$, RAW can be reduced to [46]

$$I_{ip}^{RAW} \approx \frac{a_{ip}}{b_{ip}} + 1 \tag{33}$$

RAW can be used to measure the relative impact of failure of a component to the sequence top event frequency, which can also be considered the consequence of the component failure. RAW can also be used to measure the importance of bringing a component back to functional state after a failure. However, RAW does not consider the duration or probability of the failed state of a component. This can be seen from the equation (33), where the BE probability is not included. RAW value of a BE is little dependent on the BE probability and more dependent on system configuration. A high RAW value indicates a weak defence-in-depth for failure of the component and the value could be decreased by for example adding another redundant component. Two events connected to an OR-gate have identical MCSs when the event itself is excluded from the MCSs. Therefore, the RAW values for such events are very similar, but not completely identical.

RAW for all operating modes is calculated similarly to FV as a weighted average [39]:

$$I_{ip}^{RAW} = \frac{\sum_p (I_{ip}^{RAW} f_{TOP,p})}{\sum_p f_{TOP,p}} \tag{34}$$

Where $\sum_p (I_{ip}^{RAW} f_{TOP,p})$ is the sum of the operating mode specific RAW values multiplied by the operating mode specific top event frequency and $\sum_p f_{TOP,p}$ is the total top event frequency.

4.1.1.4 Birnbaum importance measure

Birnbaum importance measure (BI) is considered the first RIM and it was introduced by Birnbaum in 1969 [54]. Birnbaum introduced both a structural importance (SI) and reliability importance, the latter being referred to as BI in this thesis. SI is defined as a ratio between the number of system states where component is critical to the system failure and the total number of possible system states. A component is considered critical when the system is in such state that the component failure would lead to system failure. [54] Applied to nuclear PRA, this means that the plant is in such a state that component failure would lead to core damage, i.e. all the other events in an MCS containing the event have occurred. Because of the definition, calculation of SI does not require knowledge on event parameters and the value is based on deterministic information.

BI is defined as the probability that the system is critical with respect to component failure and it is calculated as the difference between system failure probability when component

failure probability is equal to unity, and when it is equal to zero. [54] For nuclear PRA this is the frequency in which a component is challenged to function in order to prevent the sequence top event from happening [55]. Applying the calculation method of BI to nuclear PRA yields

$$I_{ip}^{BI} = f_{TOP,p}(Q_{ip} = 1) - f_{TOP,p}(Q_{ip} = 0) \tag{35}$$

BI can have values in range $[0, \infty)$ and the unit is $\frac{1}{year}$. According to equation (35) the value of BI is also the change in sequence top event frequency when the component state changes from functioning to failed. Because $f_{TOP,p}$ is a linear function of Q_{ip}, BI can also be expressed as the partial derivative of $f_{TOP,p}$ with respect to Q_{ip} as it is defined in [40]

$$I_{ip}^{BI} = \frac{\partial f_{TOP,p}}{\partial Q_{ip}} = \frac{\partial(a_{ip}Q_{ip} + b_{ip})}{\partial Q_{ip}} = a_{ip} \tag{36}$$

Therefore, another definition used for BI is the partial derivative of the total risk with respect to BE probability [56]. As can be seen, the value of BI does not depend on the probability of a BE. The value depends on the MCSs that the event is included in, and the probabilities and frequencies of all the other events in the MCSs. Events that are not included in the MCSs have no impact on the value of BI. Therefore, events under the same OR-gate should have identical BI values. Like RAW, BI is a measure of redundancy for a component failure. A small value of BI implies a high level of redundancy for the component failure and a high value of BI implies a low level of redundancy.

BI can also be calculated as a function of FV and BE probability. This is used in Loviisa PRA model to calculate the BI values for both BEs and IEs [39].

$$I_{ip}^{BI} = \frac{I_{ip}^{FV}}{Q_{ip}} f_{TOP,p}(\text{base}) \tag{37}$$

Applying equation (35) for the total top event frequency including all operating modes would yield

$$I_i^{BI} = \sum_p f_{TOP,p}(Q_{ip} = 1) - \sum_p f_{TOP,p}(Q_{ip} = 0) = \sum_p I_{ip}^{BI} \tag{38}$$

Therefore, BI across all operating modes can be calculated as a sum of operating mode specific BI values.

4.1.1.5 Differential Importance Measure

Differential Importance Measure (DIM) was introduced in [57]. DIM has two interpretations DIM_I and DIM_{II}. Both of them are based on the idea of increasing a BE or an IE parameter by a small amount and calculating the change in total top event frequency. The change in risk is compared to sum of all changes in risk when all events are individually adjusted by the same amount. For calculating DIM_I the parameter is increased by a small absolute amount. [57]

$$I_{ip}^{DIM_I} = \frac{\frac{\partial f_{TOP,p}}{\partial x_{ip}}}{\sum_i \frac{\partial f_{TOP,p}}{\partial x_{ip}}} \tag{39}$$

Where x is the parameter that is being changed. For BEs, this parameter can be any of the parameters that the BE probability is calculated from, or the BE probability itself. For calculating DIM^{II}, the parameter is changed by a fraction of its base value. [57]

$$I_{ip}^{DIM_{II}} = \frac{\frac{\partial R}{\partial x_{ip}} x_{ip}}{\sum_i \frac{\partial R}{\partial x_{ip}} x_{ip}} \tag{40}$$

Because of how DIM is defined, the sum of all DIM values calculated for BEs or IEs is 1 [57].

$$\sum_i I_{ip}^{DIM_I} = \sum_i I_{ip}^{DIM_{II}} = 1 \tag{41}$$

Another result of the definition of DIM is that it is summative, the values can be added up to calculate the DIM value for multiple events [57]. Currently there are some inconveniences related to calculating DIM. Firstly, calculation of DIM for parameters that the unavailability is calculated from is impossible. Calculating DIM on that accurate parameter level would require that the sequence top event frequency is in parameter form. Secondly, DIM is not built in any PRA software. [48] However, DIM can be calculated as a function of FV. DIM_I can be calculated as described in [56]:

$$I_{ip}^{DIM_I} = \frac{\frac{I_{ip}^{FV}}{x_{ip}}}{\sum_i \frac{I_{ip}^{FV}}{x_{ip}}} \tag{42}$$

and DIM_{II} as

$$I_{ip}^{DIM_{II}} = \frac{I_{ip}^{FV}}{\sum_i I_{ip}^{FV}} \tag{43}$$

This enables the calculation of DIM for BEs without rerunning the PRA model with new adjustments. Calculation of DIM_{II} as a function of FV implies that the ranking by DIM^{II} is equal to ranking components by their FV values, because the numerator is equal for every BE [56]. Ranking by DIM_I is also identical to ranking BEs by $\frac{I_{ip}^{FV}}{Q_{ip}}$. When considering the parameters in equation (20) DIM_I can be expressed as

$$I_{ip}^{DIM_I} = \frac{F_{ip}^{FV}}{Q_{ip}} = \frac{1}{Q_{ip}} \frac{a_{ip} Q_{ip}}{a_{ip} Q_{ip} + b_{ip}} = \frac{a_{ip}}{f_{TOP,p}} \tag{44}$$

Ranking events based on DIM_I would then be equal to ranking by BI. Considering these factors, it can be concluded that DIM does not bring any extra utility to RIMs in classification of SSCs when it is calculated based on the RIMs that have already been calculated.

4.1.2 Importance measures for initiating events

The calculation and interpretations of RIMs differ between BEs and IEs. The differences are discussed shortly in this subsection. Equation (20) is modified to apply for IEs. The factors in the equation have different dimensions for IEs due to occurrence of IEs being measured by their frequency. The equation can now be expressed as

$$f_{TOP,p} = \alpha_{jp} f_{jp} + \beta_{jp} \tag{45}$$

where

- $\alpha_{jp} f_{jp}$ is the contribution by MCSs that include Y_j to the total FT top event frequency in operating mode p. The unit of f_{jp} is $\frac{1}{year}$ and α_{jp} is dimensionless
- β_{jp} is the contribution to FT top event frequency by other MCSs in operating mode p. The unit of β_{jp} is $\frac{1}{year}$

FV can be calculated for IEs identically as it is calculated for BEs and it is comparable with BE FV values because it is dimensionless.

$$J_j^{FV} = \frac{\mathrm{Fr}\left(\bigcup_{j \in l} M_l\right)}{f_{TOP,p}} = \frac{\alpha_{jp} f_{jp}}{\alpha_{jp} f_{jp} + \beta_{jp}} \tag{46}$$

RAW cannot be defined for IEs. For calculation of RAW, the parameter describing the occurrence of the event is set to the value that is worst theoretically possible, i.e. the maximum value. For probability, the value is 1 and for frequency it is infinity. Infinite IE frequency would imply an infinite top event frequency and thus also infinite RAW. [42]

Calculation of BI does not require setting the parameter to its maximum value if it is calculated based on Equation (41). BI can thus be calculated for IEs as

$$J_{jp}^{BI} = \frac{J_{jp}^{FV}}{f_{jp}} f_{TOP,p}(\text{base}) = \alpha_{jp} \tag{47}$$

The value is now dimensionless and can have values in range [0,1]. According to [58] when BI is calculated for IEs, it measures the conditional probability of the sequence top event given the IE. RIMs called conditional core damage probability (CCDP) and conditional large release probability (CLRP) measures the same probability, but CCDP and CLRP are calculated by assuming the IE has occurred. CCDP and CLRP are included for example in [39]. The value of BI can be used to approximate the value of CCDP when calculated on level 1, and CLRP when calculated on level 2.

$$J_{jp}^{CCDP} = \Pr\left(TOP \middle| Y_j = 1\right) \approx J_{jp}^{BI} \tag{48}$$

CCDP for multiple operating modes is also calculated differently from BI for BEs as a weighted average with operating mode duration as the weighting factor. This weighted average is used for example in the RIISI-program for Loviisa NPP [59].

$$J_j^{CCDP} = \frac{\sum_p \left(J_{jp}^{CCDP} \Delta T_p\right)}{\sum_p \Delta T_p} \tag{49}$$

Where ΔT_p is the duration of operating mode p.

4.2 Importance of SSCs and functions

The RIMs are generally calculated for BEs and IEs while safety classes are determined on different levels of SSC hierarchy. This section describes and discusses the methods for applying the RIMs of BEs to determine the importance of SSCs. First the importance of a component is discussed, then the importance of a system and finally the importance of a safety function.

4.2.1 Component importance

A component can be modelled by multiple different BEs representing the individual failures and CCFs of the different failure modes of the component. As an example, Figure 13 and Figure 14 contain the different failure modes of pump TH12D0001 in two different accident sequences. The importance of a component needs to be measured based on the multiple different BEs modelling the component. Direct comparisons between BE RIMs and the safety class of the related component would result in the less important failure modes of a component being compared to the safety class the component has because of its most important failure modes. The safety classification depends on the most important functions of the component. Therefore, considering the objective of this thesis, such comparisons are not preferable.

RiskSpectrum has a built-in ability to calculate RIMs for a group of BEs. The calculation is based on setting the probabilities all the events below the gate that represents the component as unity or zero. This includes also setting probabilities of the CCF events as unity or zero. [42] This method can be considered overly conservative. This kind of calculation does not include minimization of the MCSs based on the new conditions and therefore the cut set representation may not be minimal anymore.

There are multiple alternate methods for calculating component importance based on the RIMs calculated for BEs. In Chapter 5 of this thesis, the RIM values of all components in the model are considered when the RIM values are compared to the safety classes. Therefore, it is not beneficial to require recalculating the whole model for calculating the importance of each component separately. Next, some of methods for calculating RIMs on component level are discussed. DIM is not included in this subsection due to the additivity being described already in the previous section when DIM was introduced.

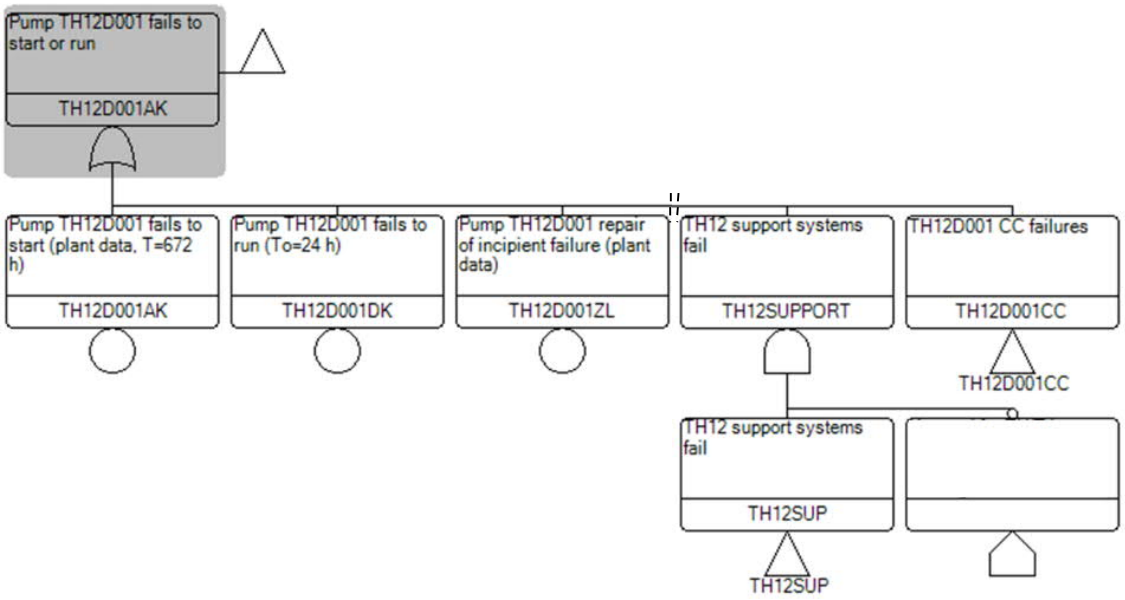


Figure 13 Failure of pump TH12D0001 to start or run

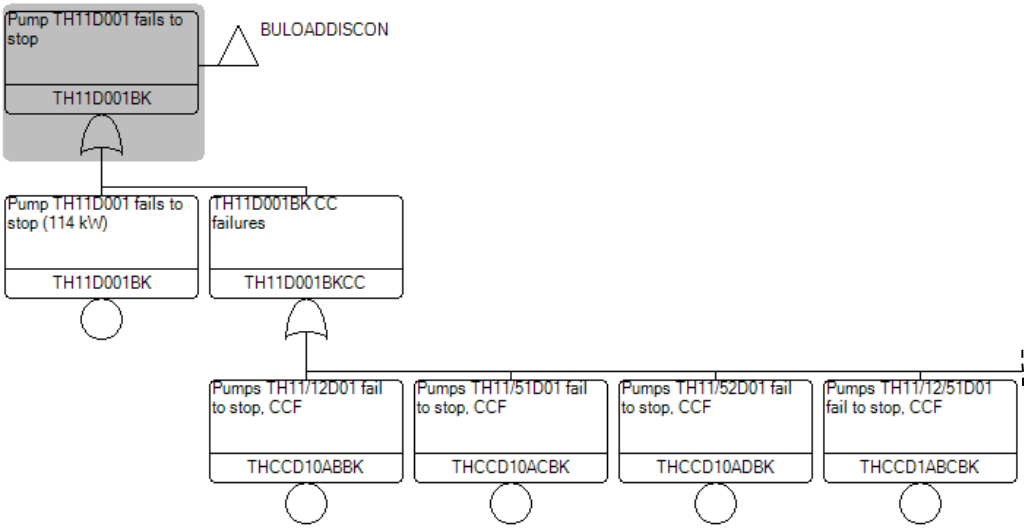


Figure 14 Failure of pump TF12D0001 to stop

4.2.1.1 Component FV

The calculation of FV for a component is relatively straightforward. Because calculation of FV does not require changing the unavailability of any component, applying it for multiple events is simple. FV is defined on component level as the share of sequence top event frequency contributed by the MCSs that include at least one of the events modelling the component. [50] In this thesis, Z_k is used to refer to the set of BEs that model component k and K_k is used to refer to the importance of the component.

$$K_k^{FV} = \frac{\mathrm{Fr}\left(\bigcup_{i\in k, i\in l} M_l\right)}{f_{TOP,p}} \tag{50}$$

Where $\mathrm{Fr}\left(\bigcup_{l|i\in k, i\in l} M_l\right)$ is the total frequency contributed by the MCSs that include any of the BEs used to model the component. If all the MCSs only include one of the BEs in K_k, the FV values can be added up to define the FV for the component.

$$K_k^{FV} = \sum_{i \in k} I_i^{FV} \tag{51}$$

None of the MCSs should have two BEs from Z_k occurring simultaneously or else some of the MCSs will be included twice. [50] When all the BEs from K_k are under the same OR-gate, or they are included in different event trees, they should not be included in the same MCSs.

4.2.1.2 Component RAW

The calculation of RAW on component level is more complex due to the BE probabilities being adjusted for the calculations. Accurate calculation of RAW for a group of BEs is discussed in [52]. It is suggested that the RAW of a component is calculated by changing all the BEs in the group to have the same BE ID, and the probability of this event is set to unity. Then, the MCSs are solved for the whole model and the sequence top event frequency is recalculated. The new top event frequency can then be used to calculate the RAW value of the group of BEs. [52] However, this method would require that the whole PRA model is ran once for every component included in the model.

Five methods for calculating component RAW without having to rerun the model are collected in [60]. In the first one the component RAW is defined to be the sum of all RAW values for the related BEs, including CCFs [60]. BEs under the same OR-gate generally have the same RAW and this method would result in multiplying that RAW value by the number of Bes. Considering that the minimum value of RAW is 1, this method would result in the total RAW of the pump in Figures 13 and 14 to be at least 3 when only the failure events are considered for the calculation of RAW.

In the second method RAW is defined to be maximum of all the related BE RAW values, including CCFs. The third method is like the second one, but CCFs are ignored. In the fourth method, two values for RAW are determined: maximum of the individual failures and maximum of the CCFs. [60] Ignoring the CCF events when considering the maximum component RAW would result in large underestimations of the component importance. Due to redundancy the importance of a single pump can be very low, but the importance of the group of the pumps can be very large. Therefore, when considering the maximum RAW values it is beneficial to consider the maximum RAW of individual failures and CCFs separately.

The fifth method is called balancing method, and in this method the component RAW is calculated based on the component FV. Balancing method utilizes the additivity of FV values and the connection between the FV and RAW values. The RAW of a component is calculated as [60]

$$K_k^{RAW,bal} = 1 + \frac{K_k^{FV}\left(1 - Q_k(\text{base})\right)}{Q_k(\text{base})} \tag{52}$$

Where K_k^{FV} is the FV-importance of the component calculated as sum of all FV values of the events modelling the component, including CCFs. Q_k is the total failure probability of

the component and it is calculated as the sum of all BE probabilities modelling the component. [60]

$$Q_k = \sum_{i \in k} Q_i \tag{53}$$

Another method based on balancing approach is called the weighted average method and it was introduced in [61]. In this method, RAW is calculated as a weighted average of BE RAWs with their probability as weighting factor.

$$K_k^{RAW,wam} = \frac{\sum_{i \in k} \left(Q_i I_i^{RAW} \right)}{\sum_{i \in k} Q_i} \tag{54}$$

It is also noted in [61] that the values of both methods are very similar for a union of mutually exclusive BEs modelling a single component. While Loviisa PRA model has no BEs set mutually exclusive, the events generally exist in different MCSs due to them being located under a shared OR-gate, or being used in different accident sequences.

4.2.1.3 Component BI

It is shown in [56] that the definition of BI as a partial derivative of risk with respect to BE probability cannot be extended to apply for multiple BEs, because partial derivatives are calculated for one variable at a time. When considering the top event frequency as a function of multiple BEs, there are multiple BE probabilities used as variables. [56] Therefore, it is suggested to use DIM_I instead of BI for ranking components by the sensitivity of the top event frequency to changes in the component failure probabilities. [56]

[56] discusses BI based on the definition as a partial derivative. However, if the definition based on system criticality was considered instead, maximum BI values could be selected for a component, analogously to selecting maximum RAW values. Maximum BI value of a component individual failures would then show the frequency in which the system is critical with respect to the most frequently challenged failure mode of the component. Maximum BI value of the CCF events would show the frequency in which the system is critical with respect to the CCF group. When the BEs are connected to a single OR-gate, they all have approximately the same value of BI. The total probability of at least one of the BEs occurring would then be the probability that the component fails when challenged. For the pump in Figure 13 the total probability that the pump fails to start or run is the sum of the probabilities of events TH12D001AK, TH12D001DK and the probabilities of the CCFs. But the total probability of failure of all the four pumps would be a more complex process to calculate.

4.2.2 System and safety function importance

While there is plenty of literature about the importance on component level, there are a lot less studies on the importance of a system. In addition, according to [62] there are no widely accepted definitions for system importance. It is also discussed that an FV-like measure could be defined for the system by calculating the sum of all MCSs that include an event modelling the system failure. A BI-like measure could be determined for the system to measure how often the system is critical. [62]

An RRW-like or FV-like measure could also be calculated for the system by setting all the probabilities of events modelling the components in the system to zero and recalculating the model and comparing the new top event frequency to the old one. Also, an RAW-like measure could be calculated by setting the probabilities to unity. For correct minimization of the MCSs the event IDs of each such event should be changed to be identical with each other. Similarly, the BI-like measure could be defined based on the reduced and increased top event frequencies. Additivity of FV values requires that the BEs do not exist in the same MCSs. Many components in a system are redundant and therefore their failure events share some of the MCSs. Therefore, additivity of FV cannot be directly applied to calculate the system FV based on the BEs modelling the system components. Instead, every MCS should be tested individually whether they include one or more events modelling the group or not. Similarly, the weighted average method and balancing method for calculating RAW cannot be extended to apply to systems because the methods include similar assumptions.

A system can be used for executing multiple different safety functions. The deterministic safety class of a system depends on the most important function it is used to execute. Assuming total failure of the system by setting all the probabilities of events related to the system to unity assumes that the system is unable to perform any of the functions it is required to. Only setting the events related to the most important safety function to unity only assumes the failure of the most important safety function. Identifying events that prevent the system from executing its most important functions can be used to solve the RAW value for the failure of the system to execute the specific function. Use of the RAW values of such events avoids having to recalculate the model to measure the importance of every system and every function separately.

It was suggested in [4] that the importance of a system for risk-informed safety classification can be determined based on the most important component of the system. The RIMs used were CCDP and event probability. CCDP of the system was approximated as the CCDP of the most important component, and system failure probability as the sum of failure probabilities of each component that can cause the system failure. [4] When using FV and RAW as the RIMs, an analogous method would be to determine the system RAW as the maximum RAW of the BEs that model the system and system FV as the maximum component-level FV of the components in the system.

Safety function importance is also discussed very little in literature. If the PRA model structure includes safety functions as gate events, then setting this gate event to TRUE or FALSE and recalculating the model would provide the increased or decreased top event frequency. The components modelled by BEs can be common to multiple different safety functions and therefore adjusting their probabilities would result in the failure probability of the other safety functions being changed too. For example, out of 5673 OLs listed in [63], 3427 (60%) OLs are common to more than one safety function.

4.3 Selection of importance measures for the comparison

RIMs generally measure the component importance from two different perspectives. A division of RIMs into two categories is used in [52] where it is described that they either measure risk or safety significance. An SSC is considered risk significant if the imperfection of the component contributes significantly to the CDF or LRF. Safety-significance is related to the role that an SSC has in prevention of accidents. [52] RIMs included in this thesis that

measure risk significance include FV, RR, and RRW. RIMs that are used to measure safety significance include RA, RAW, BI and CCDP and CLRP.

A common aspect for the risk significant RIMs is that their values depend on the probability of the event in question. The values of safety significant RIMs are little or not at all dependent on the probability. However, due to the cutoff limit, all the RIM values are also affected by the event probability to some degree. When considering equation (20), the values of risk significant RIMs are dependent on the term $a_{ip}Q_{ip}$, and the values of safety significant RIMs are dependent only on the term a_{ip}. The safety significant RIMs are therefore only dependent on the system structure.

While the RIM values itself carry a lot of information, their relative rankings are the more important when considering their categorization. On BE level the risk significant RIMs all provide very similar rankings for the events. However, some deviations should exist due to how the values are rounded differently.

Similarly, BI and RAW should yield very similar rankings. As shown by equations (36) and (44), RAW is slightly dependent on the BE probability whereas BI is not dependent on the probability at all. Therefore, there should exist some differences between the rankings even if the values were calculated to a larger number of significant digits. Figure 15 plots the rankings of BEs by their RAW and BI values in power operating mode. There is a clear correlation between the two ranks, but at higher ranks the effect of rounding of RAW values can be seen. On component level the rankings would then also be similar if the same methods are used to determine the component level BI and RAW. While the rankings are not completely identical, using both RAW and BI instead of only one of them would not bring much additional value to the identification of component significance.

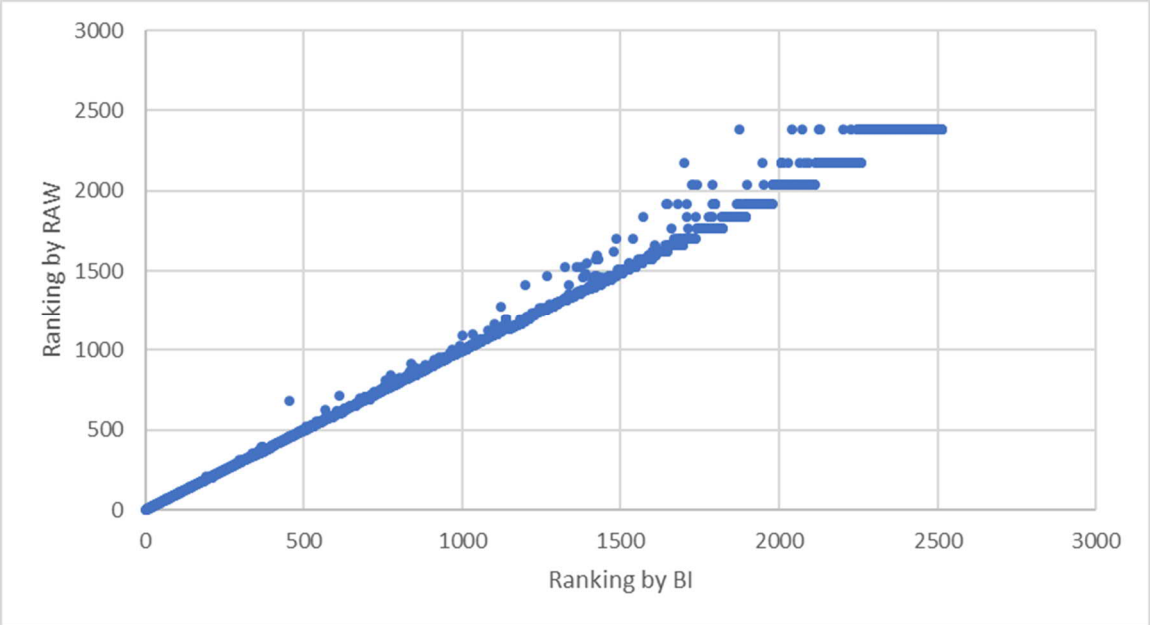


Figure 15 Rankings of BEs by their BI and RAW values during power operating mode. BEs with either $I_i^{BI} = 0$ or $I_i^{RAW} = 0$ were ignored.

Both the risk and safety significance of an SSC should be understood when considering the safety classification of the SSC and this requires the use of at least two RIMs. A common

combination of RIMs used widely in literature is FV and RAW. This combination is also used for risk-informed safety categorization in the United States as described in Section 4.5. There are also multiple studies for the use of FV and RAW to measure the importance of a component that is modelled by multiple different BEs. This combination will also be used in this thesis to measure the risk and safety significance of components based on BEs. RAW cannot be calculated for IEs and therefore the CCDP is used instead when considering the safety significance based on the IEs a component can cause.

4.4 Effect of safety class on importance measure values

The RIMs are all functions of system structure, while some RIMs are also affected by the failure probability of the event in question. While the RIM value may not be affected by the probability of the event itself, the probability still has some effect to the importance of other events that belong to some of the same MCSs. In this section the requirements that are set in YVL-guides based on the safety class and the impact the requirements can have on the RIM values are discussed.

The system structure has a large impact on which events an MCS consists of. [15] covers requirements on plant and system design. This includes requirements for system configuration, such as requirements on separation and failure criteria of components. However, the failure criteria are based on safety functions and what they are designed to achieve, rather than being based on the safety class. For example, systems that are designed to bring the plant to controlled state and maintaining the controlled state after a severe accident need to fulfil (N+1) failure criterion. While such systems are classified to SC3, it is not a direct consequence of the safety class of the systems. There are also requirements that do not specify a specific safety class, instead they are applied for all safety classified SSCs of a specific kind. For example, there should not be cross-links between safety classified redundant electric systems unless the links are beneficial for safety.

YVL E -guides [64] include requirements for NPP structures and components. The following guides include requirements that directly affect the safety classified components:

- YVL E.3: Pressure vessels and piping of nuclear facility
- YVL E.5: In-service inspection of nuclear facility pressure equipment with non-destructive testing methods
- YVL E.7: Electrical and I&C equipment of a nuclear facility
- YVL E.8: Valves of a nuclear facility
- YVL E.9: Pumps of a nuclear facility
- YVL E.10: Emergency power supplies of a nuclear facility
- YVL E.11: Hoisting and transfer equipment of a nuclear facility

The failure probabilities of components are functions failure rate, test run interval and repair rate as shown in equation (1). The test run interval usually causes the largest share of the total unavailability. If the interval is halved, the unavailability is also approximately halved. This also leads to ~50% reduction in the frequencies of all the MCSs that the component is included in. If a real-time monitoring can be added for the component, the share of unavailability caused by the test run interval is practically eliminated. There are some requirements that affect the test run intervals of safety classified components, but the interval does not completely depend on the safety class. Some less important components are tested at the same time as other more important components are tested due to this being more

practical than to test them on separate intervals. The intervals have also been adjusted based on the PRA results.

The other time-related factor of equation (1) is the repair rate. This is primarily affected by the allowed repair times set in operating limitations and conditions [36]. These allowed repair times set an upper limit for the time in which the failure must be repaired. The repair times are mainly determined based on the failure criterion of the system and partly on PRA results, therefore safety class has little impact on the allowed repair times. [36]

There are also requirements on the supplier of the component, standards that are followed, structure and material design of the component, construction planning, testing, installation, maintenance and spare parts. The factor that such requirements have the greatest effect on is probably the failure rate. While the safety class has an effect on the selected maintenance program, or programs, the programs in Loviisa NPP are also guided by a criticality class that is set separately from the safety class. The criticality class depends on aspects such as availability requirements, safety requirements, requirements by official and maintenance costs. Therefore, the effect the safety class has on failure rate through maintenance requirements is not clear. The maintenance programs include:

1. Preventive maintenance (based on time)
2. Condition based maintenance (based on condition monitoring)
3. Corrective maintenance (component is operated until failure)
4. Curative maintenance (aspects that can improve availability, maintainability and organization performance are selected to improve the availability of the components by optimizing O&M costs)

There have been few studies on the effect of safety class on the failure rate. In [65] the failure rate difference between SC3 and commercial-grade components were set to be compared, but it was found that the methods for collecting failure data were fundamentally different in NPPs and in other industries. [65] Some values for failure rates of safety classified components can be determined based on the failure data of components in Loviisa PRA model. Figure 16 includes some values calculated from the failure rates of valves whose failure rate is determined based on plant data. There is no direct connection between the safety class and failure rate identifiable from this data. The failure rate also depends on multiple other factors, such as where the valve is located in the plant, what kind of conditions it is operated at and how it is operated. However even if the calculational failure rate is little affected by the safety class, the higher standards help ensure for example new spare parts are also high quality and the component will not fail due to weak spare parts when repaired.

There are many other factors that affect the failure probabilities in addition to the safety class of a component. Therefore, identifying the effect that the safety class has would be a very complex process. When considering the RIM values, the source of data also has a great factor on the value of failure rate. Generic data tends to be more conservative, while plant data is more accurate. Therefore, there is much variance in amount of conservativity and uncertainty of the failure rates. There are also negative aspects about changing the current safety class considered in [66], including increased requirements on the spare parts, that may increase the repair times and make finding suppliers more difficult [66]. It can be concluded that while both safety class and RIM values depend on the component and its location within the plant, the safety class has no direct influence on the RIM values.

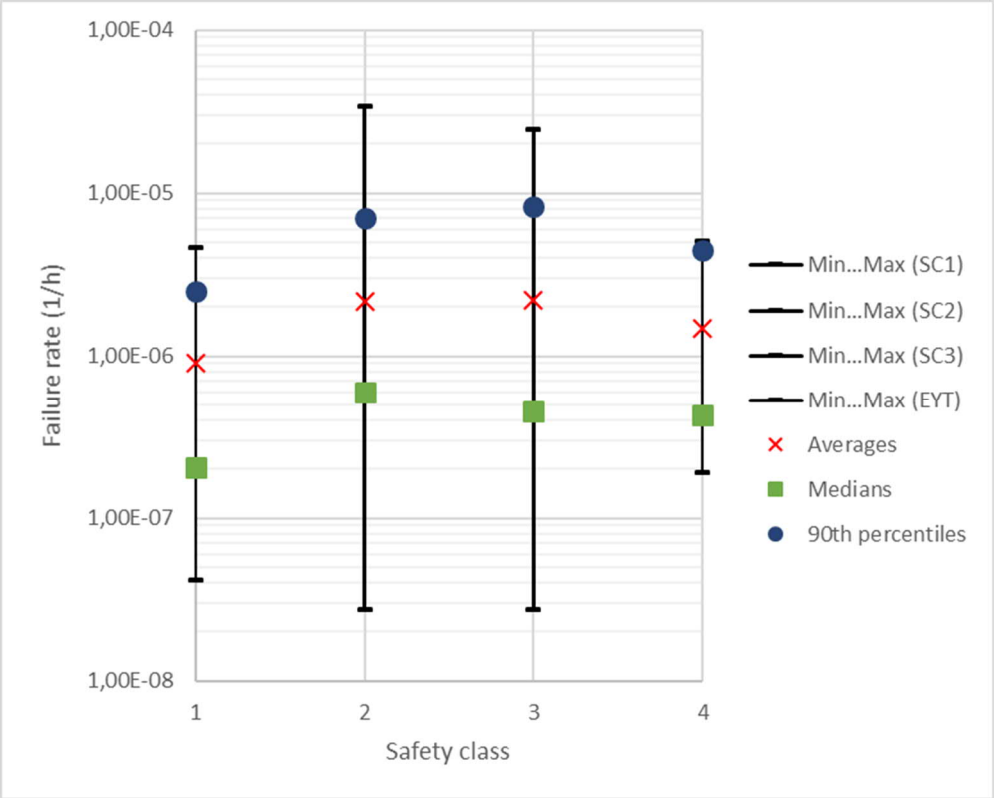


Figure 16 Failure rates of valves in the PRA model whose failure rate is determined based on plant data, and their safety classes. Class 4 on x-axis refers to the class EYT. The used data is based on the data whose collection is described in Chapter 5.2

4.5 Risk-informed safety categorization in USA

While STUK has not provided detailed instructions on use of PRA in safety classification, PRA has been utilized for risk-informed safety classification in the United States. In 2004, the U.S. Nuclear Regulatory Commission (NRC) introduced rule 10 CFR 50.69 [67] that enabled the use of PRA for risk-informed safety categorization of SSCs. U.S. Nuclear Energy Institute provided guideline NEI 00-04 [68] as instructions on how to perform the safety categorization by utilizing RIMs calculated with PRA. The objective of the rule 10 CFR 59.69 was to relax the requirements on less important SSCs that do not significantly affect the risk while identifying SSCs that have a significant effect on the safety [69].

Prior to 10 CFR 50.69 the SSCs were categorized into two safety classes based on deterministic methods. The classes were safety-related and non-safety-related SSCs. Safety-related SSCs are defined as SSCs that are required to remain operational during design basis events to secure the integrity of reactor coolant pressure boundary, to shut-down the reactor or to mitigate the consequences of accidents. 10 CFR 50.69 did not replace the two classes, but rather divided both categories into two subcategories. Safety-related SSCs were classified to risk informed safety classes RISC-1 and RISC-3, while non-safety-related SSCs were classified to classes RISC-2 and RISC-4. [68] The official definitions for the classes from [67] are:
9

- RISC-1: safety-related SSCs that perform safety significant functions
- RISC-2: non-safety-related SSCs that perform safety significant functions
- RISC-3: safety-related SSCs that perform low safety significant functions

- RISC-4: non-safety-related SSCs that perform low safety significant functions

Here, the safety significance is used to refer to both kinds of significance described in the previous subsection. One part of determining whether or not an SSC is significant includes comparing the FV and RAW values calculated from plant-specific PRA to values provided in [68]. When considering the FV and RAW limits, the FV-RAW plane is divided into two sectors as illustrated in Figure 17. The limits for identifying candidate safety significant SSCs are [68]:

- Sum of FV values for all BEs modelling the SSC, including CCFs is higher than 0,005
- Maximum of RAW values for BEs modelling the SSC, excluding CCFs, is higher than 2
- Maximum of RAW values for all BEs modelling the SSC, including CCFs, is higher than 20

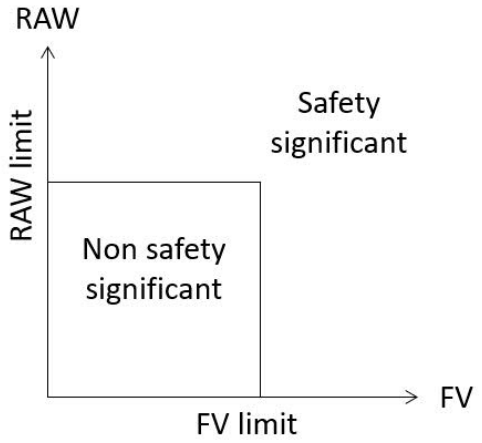


Figure 17 Dividing FV-RAW plane into two sectors with limits defined in NEI 00-04

Only one of the limits is required to be exceeded for the SSC to be considered safety significant. If the component failure can cause an IE, the FV of the IE is also compared to the FV criterion. In addition to comparing the FV and RAW values, multiple additional aspects need to be analyzed, such as operating experience and expert panel evaluations. Sensitivity studies should also be performed by adjusting the BE probabilities, such as setting all maintenance events to 0, and recalculating the model. The safety-related SSCs are mainly categorized as RISC-1, unless a strong basis for categorizing it as RISC-3 can be shown. [68] The SSCs that are not modelled in PRA are categorized completely on the basis of their deterministic importance [70]. Other criteria used to determine if a component is significant are collected in [71] and [70]. In [71] the criteria are given for FV and RAW separately, like in the American RISC, while in [70] some criteria are based on combinations of FV and RAW that both need to be exceeded. The different FV and RAW criteria from [70] and [71] are collected in Appendix 1.

Applying a similar risk-informed classification system in Finland would be analogous to dividing each of the current safety classes into two classes, resulting in total of 8 different risk-informed safety classes. Therefore, such limits cannot be directly applied to a Finnish NPP and they are not suitable to be used directly for safety classification in Finland.

5 Comparisons and suggested guiding values

In this chapter the RIM values and safety classes of components are first compared to each other based on RIMs calculated for BEs and IEs separately. This is because while most of the BEs are used to model different failure modes of individual components, IEs are used to model more general failures in larger entities, such as leakages in large piping sections of the primary circuit. Also, the CCDP and RAW values cannot be compared directly with each other. The comparisons are primarily focused on level 1 PRA, but the level 2 is also discussed briefly. Then, guiding values to be used in assistance in safety classification are suggested based on the findings from the comparison and the values are tested against the current classification. Finally, the results and potential sources of errors are discussed.

5.1 Comparison based on basic events

The comparison based on BEs is carried out in this section. The data sources and organization of data are described first, and then the component-level RIMs are compared to their safety classes and the also systems are briefly compared to the safety classes of their parts used to execute the most important functions.

5.1.1 Data

The data sources consist of two different parts: data about OLs and data from the PRA model. The data from OLs was obtained from multiple different sources listed below:

1. LOMAX asset management system [29]: KZ-IDs, descriptions, component types and safety classes of process system components and of some electrical and automation system components
2. Electrical safety classification document and its attachments [72]: missing electrical safety classes of some process system components, safety classes of electrical SSCs
3. Automation safety classification document and attachments [63]: some missing automation system OLs, missing automation safety classes of some process system components, safety classes of automation cabinets and the safety functions of all SSCs
4. LO1-K8048-00018 [66] attachments 1 and 5: Deviations between safety classes of OLs in Loviisa NPP compared to the requirements set in YVL B.2

The OL related data was collected in Excel into a worksheet with an array of all OLs and their safety classes. The highest safety class, with highest referring to the most important class, was selected to be used in the comparisons. If the safety class required by [3] was higher than the one used in Loviisa NPP according to the list in [66], the safety class required by [3] was used. This is more in line with the objective of obtaining understanding about how the safety classes defined in YVL B.2 are in line with the RIM values.

The PRA related data was also collected from multiple sources listed below:

1. PSADATA: BE IDs, descriptions, probabilities, failure rates, additional information about the event, and the source for failure data (plant data / generic data)
2. Loviisa PRA main report [39] chapter 12 attachments 1 and 2: RIMs for BEs on PRA levels 1 and 2

The data from PSADATA was processed first in order to select the BEs to be used in the comparison, and to associate each of them with one or multiple related OLs. Only the events were included that are related to technical failures and for which RIMs have been calculated. Recovery events related to component recoveries after failures were also ignored. The failure events were then classified as either individual failures or CCFs. A single matching OL was associated with each individual failure based on the event ID and description. If there were multiple OLs that would match the event due to multiple redundancy numbers, the one with the highest safety class was selected. CCFs were handled similarly, but now multiple OLs were associated with the event.

There are components whose KZ-ID only consists of the subsystem part of the ID. For example, switchgear 10BA11 is considered one component with respect to the safety classification. An individual switch 10BA11Q0001 is not classified separately. According to [20], rather large electrical entities can be considered components if they form a logical whole based on purchasing, installation, operation and quality assurance. There are also multiple automation cabinets that are classified on cabinet-level. Therefore, whether the component is classified on subsystem (10BA11) or component (10BA11Q0001) level was identified in addition to the OL. There are also some OLs identified in the PRA model that do not match any OLs in the Lomax system or the safety classification documents. For such events, an imaginary OL was added to the list exported from the Lomax system and the safety class for this imaginary location was selected based on the OL one level higher in the hierarchy.

An Excel-macro was created to reorganize the data into a single worksheet. The output of this macro is an array consisting of every OL modelled explicitly in the Loviisa PRA model, their safety classes and a list of BEs used to model the OL. If the classification is done on subsystem level of the KZ-ID, then the list includes the subsystem and events are selected based on the most important OL within the subsystem. The most important OL was selected based on component-level FV values. For a large share of subsystems, the most important component according to FV values was also the most important component according to RAW values. Therefore, there was no need to use two different components within the subsystem to identify the importance according to RAW and FV separately.

Two EYT systems were ignored from the comparison. These are systems that have been noted as important according to the PRA results and corrective actions have been performed in order to maintain them according to their importance without changing the safety class. In addition, the system YZ that only includes signals in the model was ignored and also all components with $K_k^{FV} = 0$ were ignored. Table 3 below shows the number of components from each safety class modelled explicitly in the PRA model. According to Table 3, the current safety class deviations from YVL B.2 primarily decrease the safety class of SSCs. The SSCs that are classified as SC1 according to YVL B.2 do not have their safety classes changed.

Table 3 Number of components of each safety class modelled in the Loviisa PRA model with BEs

Safety class	Number of components when the class is selected based on YVL B.2	Number of components when the class is selected based on classification in the plant
SC1	71	71
SC2	575	462
SC3	370	475
EYT	199	207

The BE IDs were then used to fetch the BE RIM values from their respective sheets, and the component level RIMs were calculated based on the BE RIMs. The RIMs are calculated for single operating modes, and the total RIM value can be calculated from the operating mode specific values. The power operation covers around 90% of the total time of operation, but only less than 50% of total CDF. Therefore, the RIM value that is used for a BE is selected as the maximum of either the total RIM, or the power operating mode RIM.

There are also some BEs in the model that refer to leakages in different piping sections within the system. The leakage can be caused by individual leakages in multiple different pipes in the piping section or by multiple different components in the piping line. Failure rate for leakages is determined as a sum of the failure rates of individual piping sections or components. The leakage event was added as an individual failure to each component that can cause the leakage, but the probability and FV-values were multiplied by this share of total failure rate. The RAW values are only little dependent on event probability and therefore they were not multiplied by any factor.

5.1.2 Comparison based on component importance

Next the safety classes of components are compared to the BE RIM values. The component-level FV was calculated using equation (51). Three different values of RAW were calculated for each component. Therefore, the four RIMs used are:

1. K_k^{FV} is the sum of FV values of all BEs that model both the individual and common cause failures of the component. Also referred to as ∑FV in figures and tables
2. $K_k^{RAW,single}$ is the maximum RAW value of the BEs that model individual failures of the component. Also referred to as max(RAW,single) in figures and tables
3. $K_k^{RAW,wam}$ is the RAW value according to the weighted average method. Also referred to as RAW,wam in figures and tables
4. $K_k^{RAW,all}$ is the maximum RAW value of the BEs that model both individual and common cause failures of the component. Also referred to as max(RAW,all) in figures and tables

The relationships between safety classes and RIM values can be analyzed through absolute RIM values, relative rankings and distributions. The absolute RIM values are analyzed first. Figure 18 shows the K_k^{FV} and $K_k^{RAW,wam}$ values plotted on an FV-RAW plane. $K_k^{RAW,wam}$ was selected to be used for plotting purposes because it combines both individual and common cause failures.

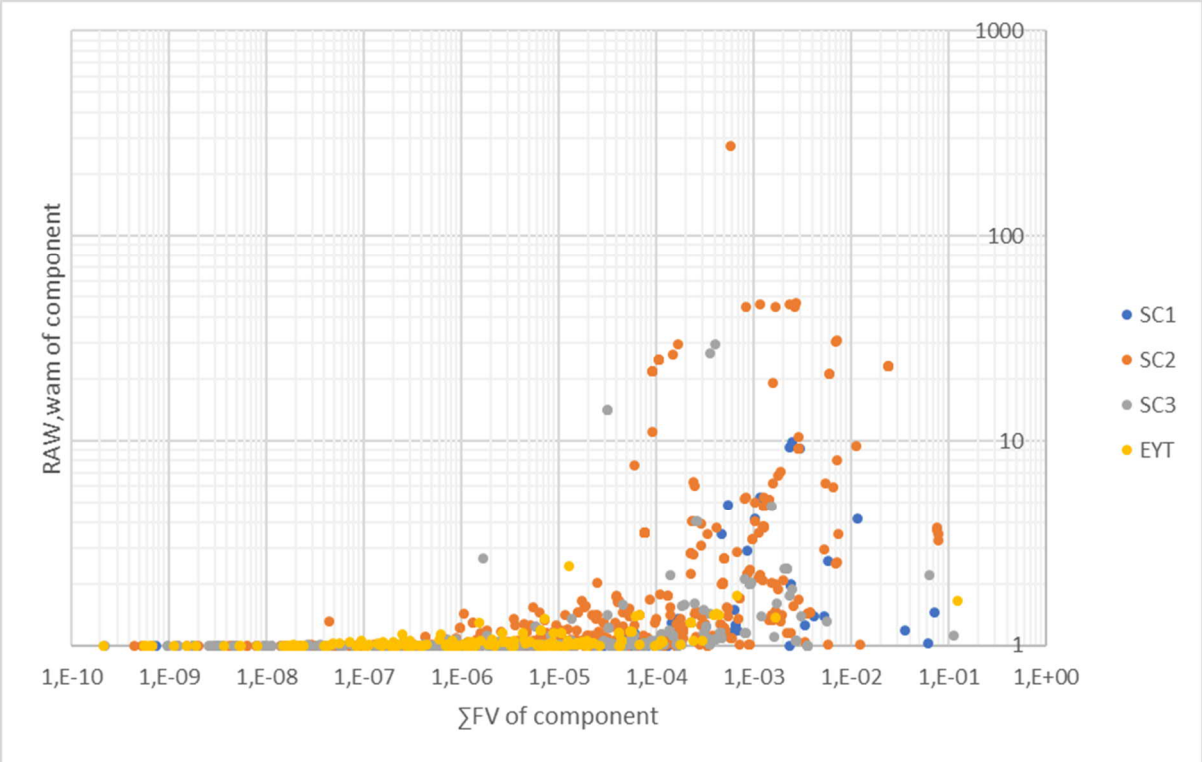


Figure 18 Components mapped on an FV-RAW plane

What can be seen from the FV-RAW plane is that the RIM values of components are not completely in line with their significance. For example, there are multiple EYT and SC3 components that are considered more significant according to their RIM values than some of SC1 and SC2 components. A component having a higher safety class than another does not always mean that it is also more significant according to the RIM values. It can also be seen that there are both SC2 and SC3 components that are considered more significant than the most important SC1 components. This is better illustrated in Figure 19 where the components are ranked according to their FV and RAW values and the ranks are plotted on plane where the x-axis is the ranking by FV values and y-axis is the ranking by RAW values. The ranks are calculated with the RANK.AVG function in MS Excel that returns the average rank of multiple SSCs if they share the same RIM value.

The effect of the rounding of RAW values can also be seen from Figure 19 where the components that rank lowest according to RAW all share the same ranking because their RAW values are very low and therefore they round down to 1,000. It can also be seen that components can rank very differently according to their FV and RAW values There are components that are ranked in top 100 based on FV, but the rank based on RAW is over 800. While a component can be one of the most likely ones to cause the sequence top event given that it happens, the consequences of one failure are not that large. It can be found by analyzing the data that components with high probability and low consequence failures rank high on FV, but low on RAW. The biggest differences in ranks are due to events with events that have probabilities that are conditional to the IE (e.g. the value is 0,5). Components that rank high on RAW, but low on FV are components with mediocre RAW and very low probability. It is also noticeable that components from each safety class include both components ranked relatively high and components ranked relatively low based on either

RIM values. The SC2 components still cover the largest share of components that rank in top 200 based on both of the RIM values.

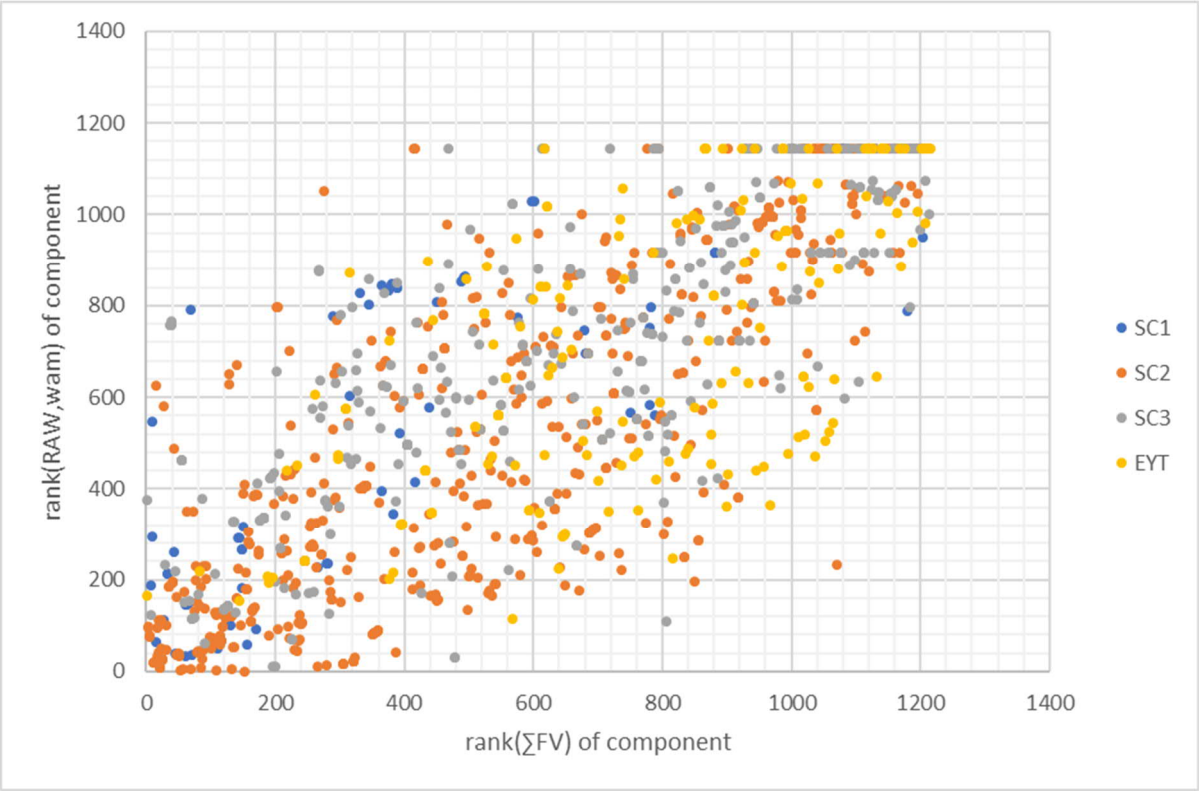


Figure 19 Relative ranking of components based on their FV and RAW values

A large share of the most significant EYT components are from the ventilating and heating systems. Some electrical components and emergency cooling towers are also included in the most important EYT components. The electrical and air conditioning systems have effects on the functioning of other systems. If the distribution centers or emergency power generators do not function, then they also cannot supply power to the other systems. If the ventilation of a room fails, then components in those rooms are also subject to potential failures. If the RIM values were taken into account in safety classification, then probably the classification of these components and their systems should be increased.

SC3 also contains some ventilation components whose RIM values are very great compared to the other components in the same class. Components classified as SC3 and that are required for heat removal from the primary circuit are also considered important according to their RIM values. Interestingly there are also multiple components that should be classified as SC2 according to [3] but are classified mechanically as SC3 in the plant and have $K_k^{RAW,all}$ values that would rank them into the top ten most important components of the plant according to $K_k^{RAW,all}$. The electrical and automation safety classes of these components are still SC2 and it is possible that reclassifying them as SC2 mechanically would not have any effect on the safety of the plant or the effect would be only minimal.

While the safety classification is not completely in line with the RIM values of the components, on average the components in higher safety classes have higher RIM values than the ones in the lower safety classes. This indicates that if two components were selected randomly from two different safety classes, the component from the higher class would be

likely to be more significant according to the RIM values. This is shown in Table 4 where measures of middle and spread are collected. The measures include maximum, average, median and the 90th percentile[1] calculated on basis of BE RIMs.

Table 4 Values calculated based on the absolute values of RIMs included in the comparison

max(RAW,single)				
Safety class	**Max**	**Average**	**Median**	**90th percentile**
SC1	78,62	4,14	1,02	8,32
SC2	275,62	3,17	1,01	1,76
SC3	29,41	1,53	1,01	1,23
EYT	2,44	1,06	1,00	1,15
ALL	275,62	2,38	1,01	1,42
max(RAW,all)				
Safety class	**Max**	**Average**	**Median**	**90th percentile**
SC1	78,62	5,62	1,13	8,79
SC2	275,62	29,40	1,26	166,29
SC3	239,87	3,59	1,01	2,94
EYT	27,10	1,31	1,01	1,30
ALL	275,62	15,55	1,04	23,48
RAW,wam				
Safety class	**Max**	**Average**	**Median**	**90th percentile**
SC1	9,85	1,78	1,02	3,51
SC2	275,62	3,27	1,06	3,88
SC3	29,41	1,33	1,01	1,30
EYT	2,44	1,06	1,01	1,17
ALL	275,62	2,23	1,01	2,23
∑FV				
Safety class	**Max**	**Average**	**Median**	**90th percentile**
SC1	7,3E-02	3,3E-03	7,3E-05	3,3E-03
SC2	7,9E-02	1,1E-03	1,9E-05	1,4E-03
SC3	1,1E-01	7,0E-04	4,2E-06	4,5E-04
EYT	1,2E-01	6,6E-04	2,2E-06	6,7E-05
ALL	1,2E-01	1,1E-03	9,1E-06	9,3E-04

The values calculated for Table 4, except for maximums, are slightly biased because the components that are modelled with BEs in the PRA model only cover a small share of the total components in the actual plant. Ratio between number of components in the model and in the actual plant is the smallest for EYT components. Therefore the averages, medians and percentiles would decrease the most for EYT components if the whole plant was modelled and the values in Table 4 were calculated based on all components of the plant. This factor needs to be noted when interpreting the values. If it is assumed that the components modelled with BEs in the PRA model are the most significant ones in prevention of IEs from propagating into accidents, then it can also be assumed that the rankings in Figure 19 are still unaffected by the lack of modelling every component in the plant. The 10th most

[1] For example, the 90th percentile of K_k^{FV} shows the value of K_k^{FV} that 10% of components within safety class exceed

important component would still be the 10th most important one. This assumption is not completely true due to there being some components that are modelled implicitly in the model.

The maximums, averages, medians and 90th percentiles are for the most part in line with the safety classification. One exception is SC1. SC1 is only used as a structural safety class and BEs are more related to failures of components to execute certain functions that are required in order to prevent the IEs from propagating into accidents. The failures of valves to open, pumps to start, etc. are usually caused by failures of their actuators to function rather than structural failures of the valves and pumps. Therefore, it can be considered that the significance of SC1 components cannot be seen that clearly from the BE RIMs. Their significance is notable when analyzing IEs that are more often related to structural failures, e.g. leakages.

When considering only SC2, SC3 and EYT components the values are in line with the safety class with the maximums of K_k^{FV} values being an exception. The maximum of SC2 is higher than the maximum of SC3. The maximums can be set by a single very significant component and therefore are not that informative. The 90th percentile is still higher for SC2 components indicating that there are only few SC3 components with FV value that high.

The RIM values can also be compared to the limits used in NEI 00-04 [68]. The resulting shares of components in each safety class that would be considered safety significant according to their RIM values are shown in Table 5. Very few components in the class EYT are considered safety significant according to the criteria, but also only around a quarter of SC2 components are considered safety significant. The percentages are in line with the safety classes of components. The share of safety significant components increases as the safety class increases. When considering the three different criteria that can set a component safety significant, the K_k^{FV} criterion is clearly exceeded by the least number of components. However, the FV contributed by the IEs is ignored here. Therefore, especially the number of SC1 and SC2 components that exceed the FV criterion may be actually higher.

Table 5 Comparison of component RIM values to the USA limits for safety significant components

Safety class	Total components	Exceed RAW,single criterion	Exceed RAW,all criterion	Exceed FV criterion	Exceed any criteria
SC1	71	23,94 %	5,63 %	8,45 %	26,76 %
SC2	575	9,91 %	19,65 %	3,83 %	26,09 %
SC3	370	3,78 %	2,16 %	0,81 %	5,95 %
EYT	199	0,50 %	0,50 %	0,50 %	1,51 %
ALL	1215	7,33 %	10,37 %	2,63 %	15,97 %

The 90th percentiles were included in Table 4. The other percentiles can be seen from Figure 20, Figure 21 Figure 22 and Figure 23 that show the distributions of components within each safety class according to each RIM included in the comparison. The distributions show the shares of components from each safety class that exceed a specific RIM value.

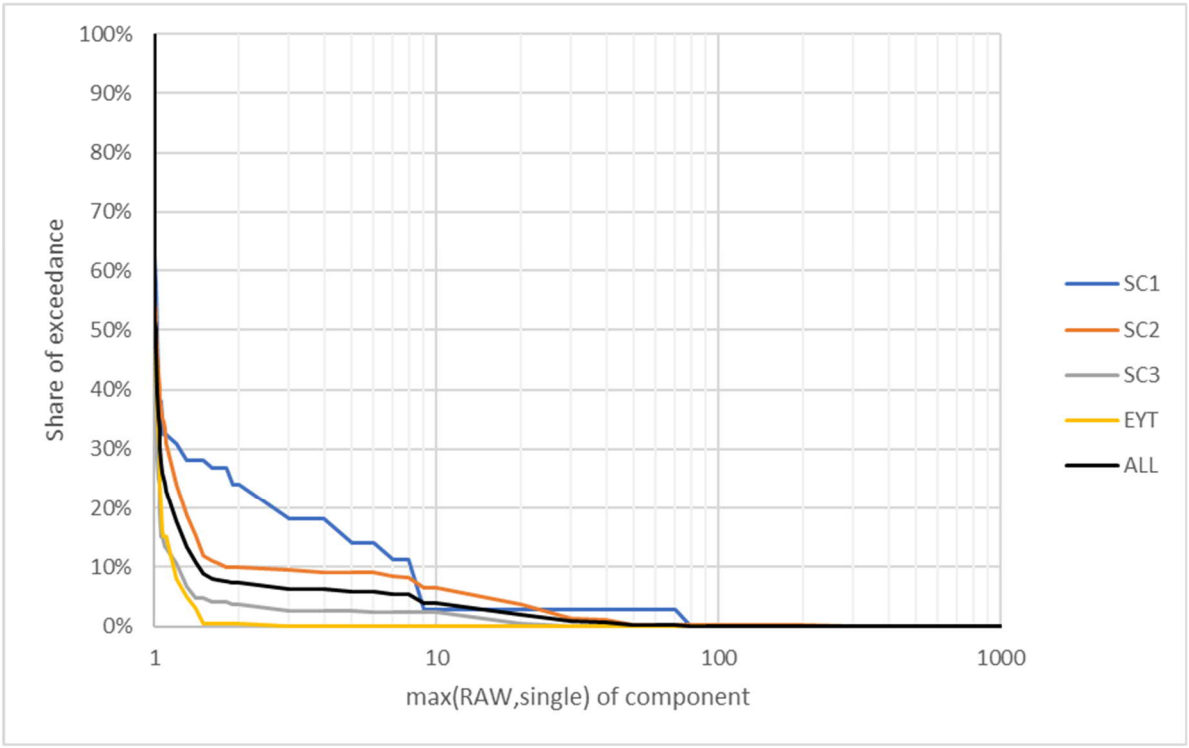


Figure 20 Distributions of component $K_k^{RAW,single}$ values

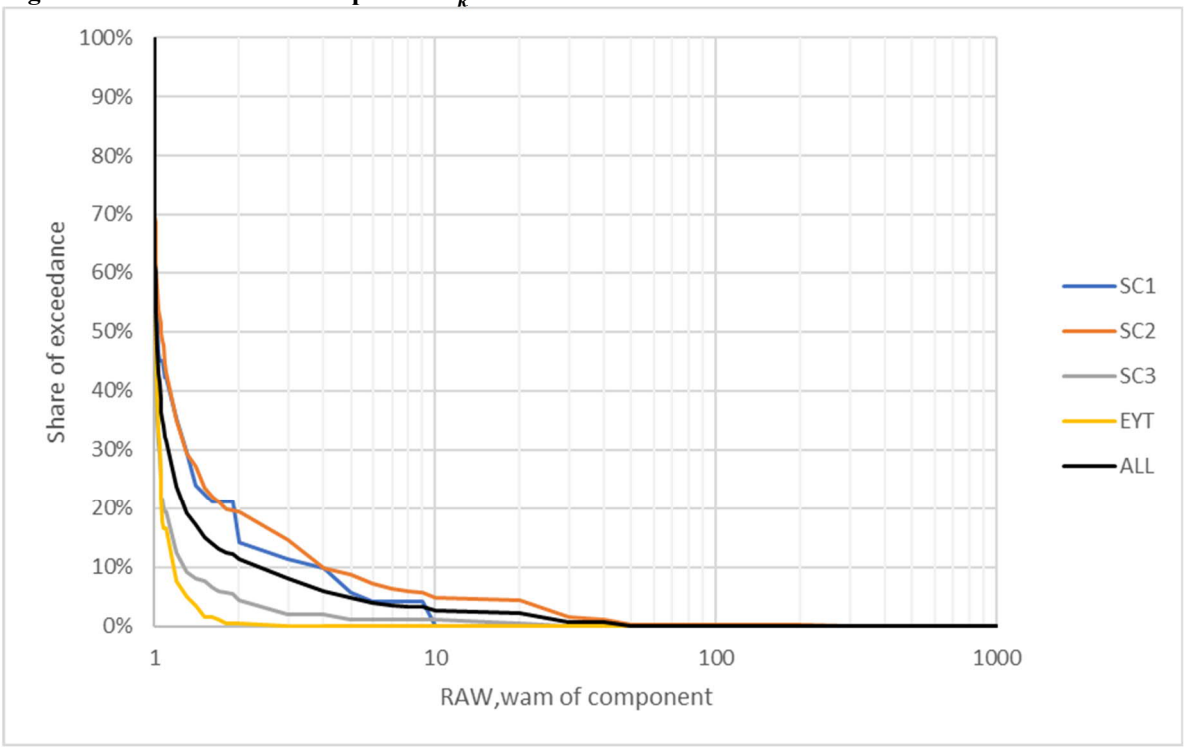


Figure 21 Distributions of component $K_k^{RAW,wam}$ values

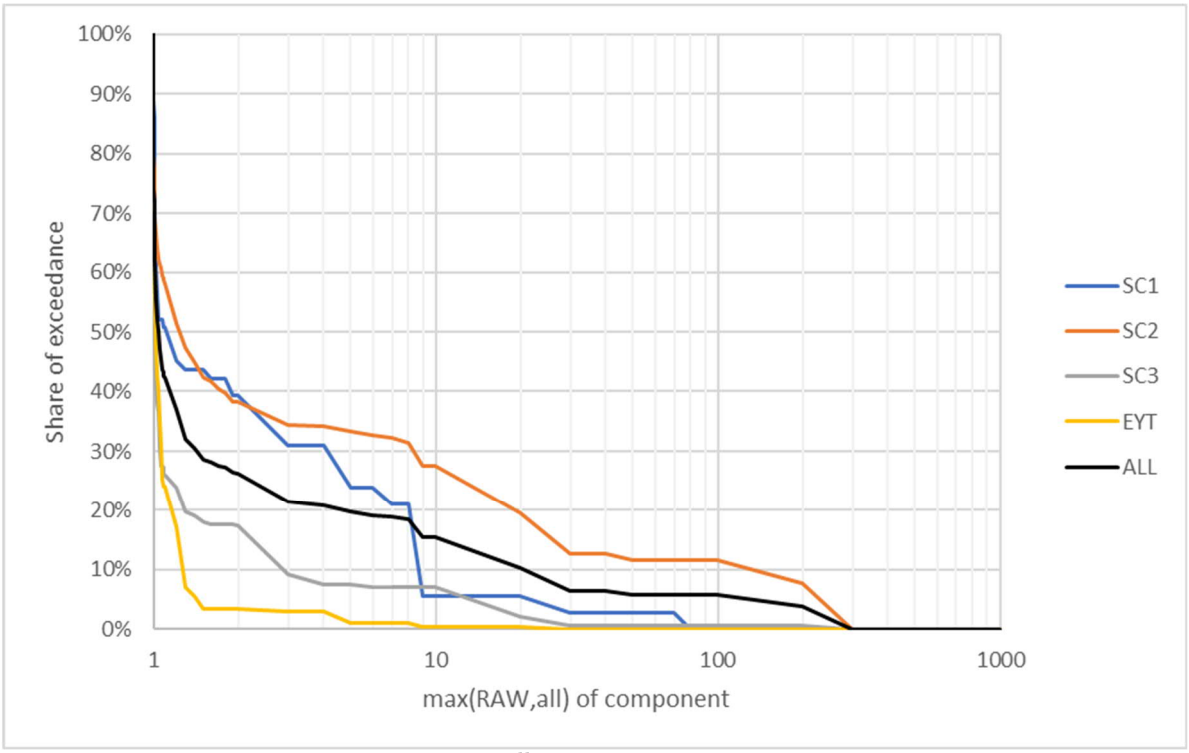


Figure 22 Distributions of component $K_k^{RAW,all}$ values

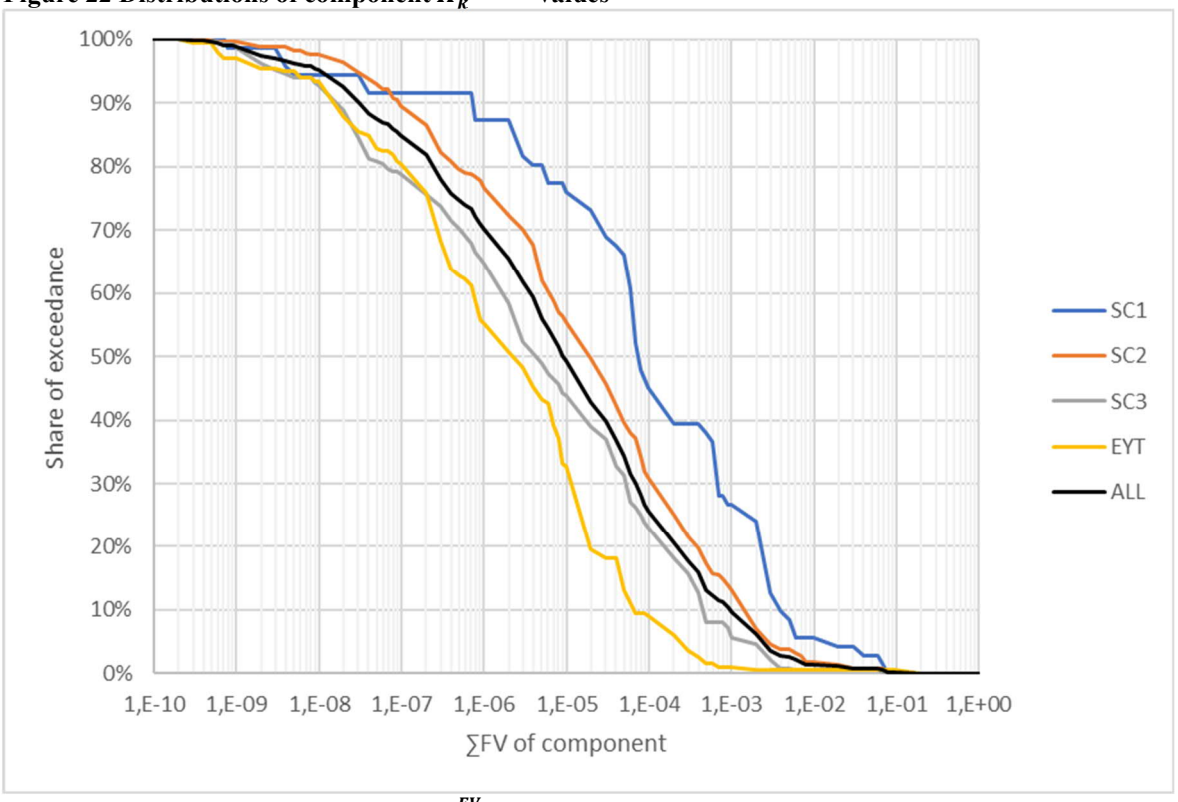


Figure 23 Distributions of component K_k^{FV} values

The distributions are also biased because only a small share of components is included in the PRA model. The effect of this can be seen in the distributions of SC3 and EYT components that are very similar based on maximum individual failure RIMs until

$K_k^{RAW,single} = 1{,}4$. If all the components of the Loviisa NPP were included in the model, then the number of components whose RIM values are equal or very close to the minimum would increase for each safety class. The curves would then be moved downwards and the EYT curves would be moved downwards the most. The differences between the distributions seem to be the smallest for $K_k^{RAW,single}$ values, but when CCFs are included in determination of component-level RAW, the differences between safety classes are more noticeable.

The safety class of a component can affect the safety classification of other nearby components due to requirements for safety class borders set in YVL B.2. Therefore, the significance of one component can have an effect on the classification of a nearby component. For example, the significance of a pump also guides the classification of a valve connected in series with the pump. In order to take this factor into account the components are grouped into approximate groups in this subsection. Doing this will ignore the less important components that are classified into higher safety classes because they are required to belong to the same class as another component.

It would be very difficult to select the exact groups of components that form groups that are required to belong into the same class. For this comparison, the components in the PRA model are grouped on basis of the subsystem-level KZ-ID, the component type (mechanical/electrical/automation) and the safety class. For example, valves 11TH20S0002 and 11TH20S0003 belong both to the group TH20,M,SC2 because they have the same subsystem ID, are both process components and have the same safety class. The RIM values for each group are now determined based on the most important components within the group according to each different RIM. Distributions of RIMs calculated for component groups are shown in Figures 24, 25, 26 and 27 below.

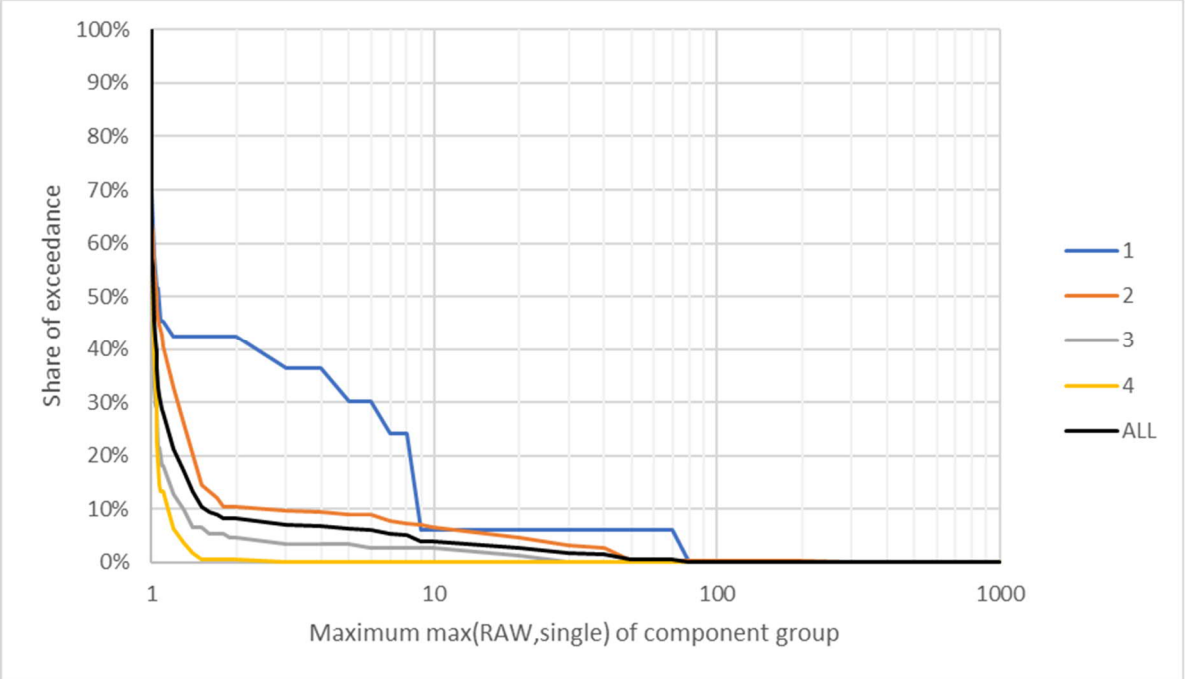


Figure 24 Distribution of maximum of $K_k^{RAW,single}$ values of component groups

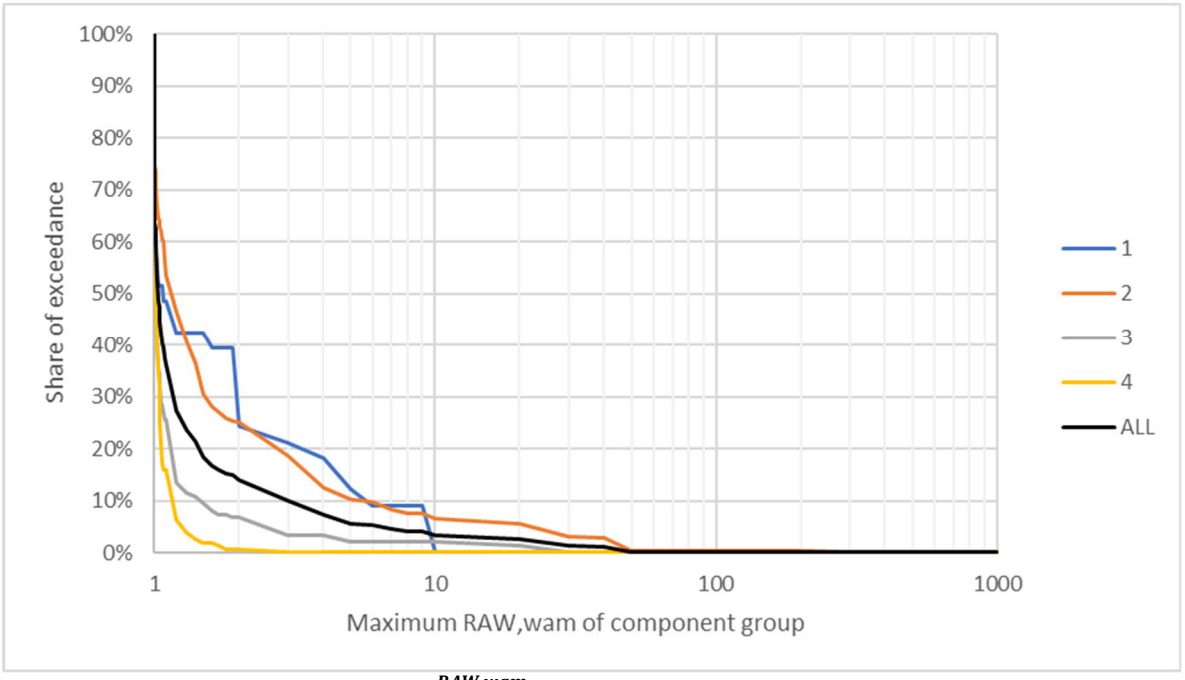


Figure 25 Distribution of maximum $K_k^{RAW,wam}$ values of component groups

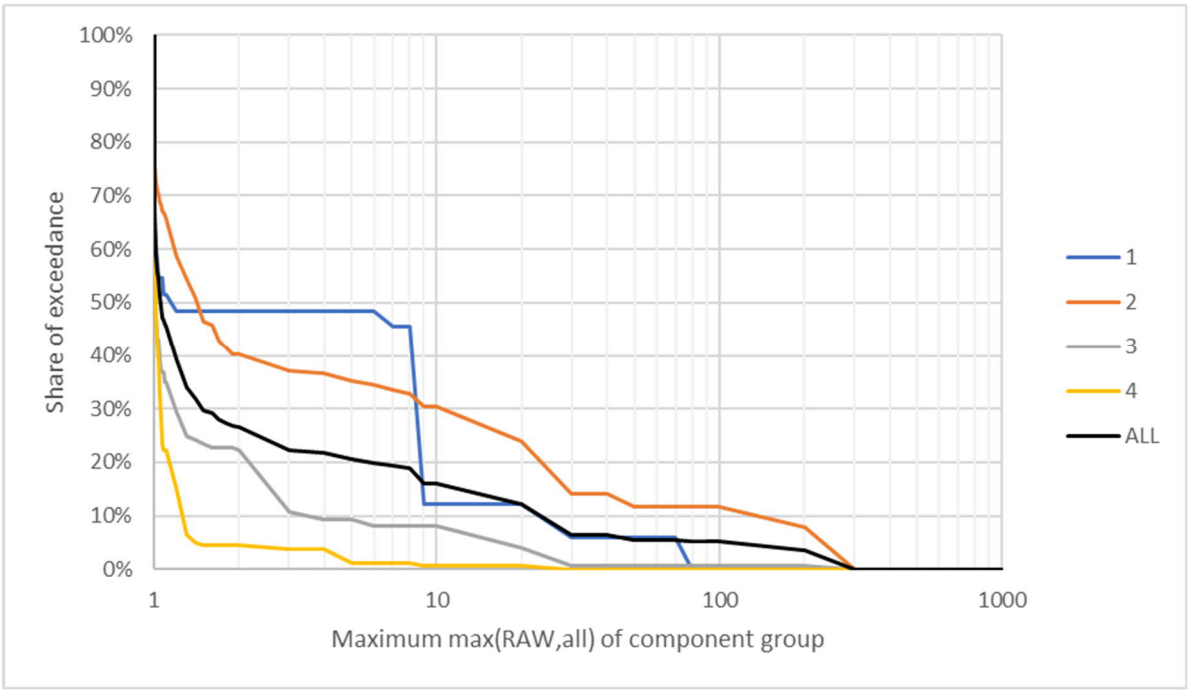


Figure 26 Distribution of maximum $K_k^{RAW,all}$ values of component groups

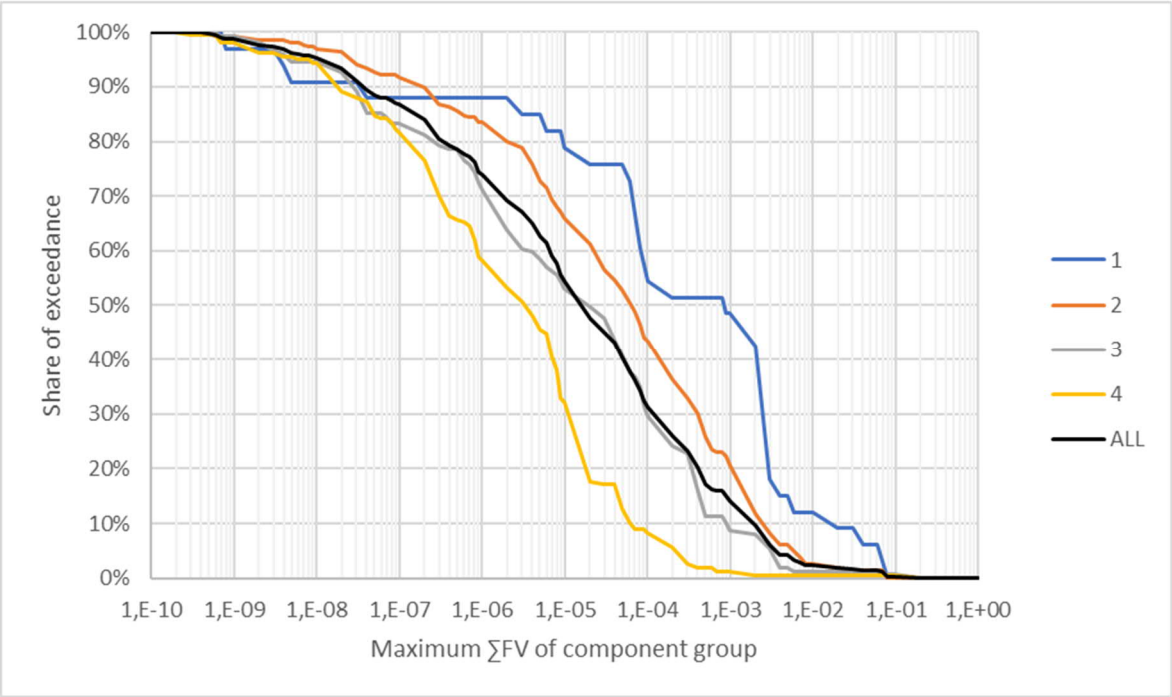


Figure 27 Distribution of maximum K_k^{FV} values of component groups

It can be seen that the differences between safety classes are greater when the component groups are used. This indicates that there are multiple less significant components in the higher safety classes that would be required to belong to these classes even if the RIM values were considered. However, there are still component groups in the higher safety classes that can be considered less significant than the component groups in lower safety classes according to the RIM values.

5.1.3 Comparison based on system importance

Next the safety classes of systems are compared to the RIM values calculated for the systems. The systems are identified based on their system level KZ-IDs. Therefore, the automation systems were ignored because the automation system hierarchy is slightly different. Because systems can consist of subsystems and components from multiple safety classes, the safety class used for a system was based on the highest safety class of the system components modelled in the PRA model. SC2 was selected as the system safety class if the highest safety class was SC1 because SC1 is not used for systems.

The FV of a system is determined based on the most significant component according to K_k^{FV} and the RAW of a system is determined based on the most significant component according to $K_k^{RAW,all}$. It was also found that for most of the systems the safety class of the most significant components according to K_k^{FV} or $K_k^{RAW,all}$ had also the highest safety class within the system. Therefore, for the most part the safety class assumed for the systems is also the safety class of the part of the system that is used to execute the system's most important functions.

The systems are shown on an FV-RAW plane in Figure 28. It can be seen that all of the most important systems belong to SC2. There is only one SC3 and no EYT systems with RAW exceeding 2. For EYT systems the maximum RAW is around 1,4. There are also some SC2

systems with very low significance, but overall, the systems from higher safety classes also have higher RIM values.

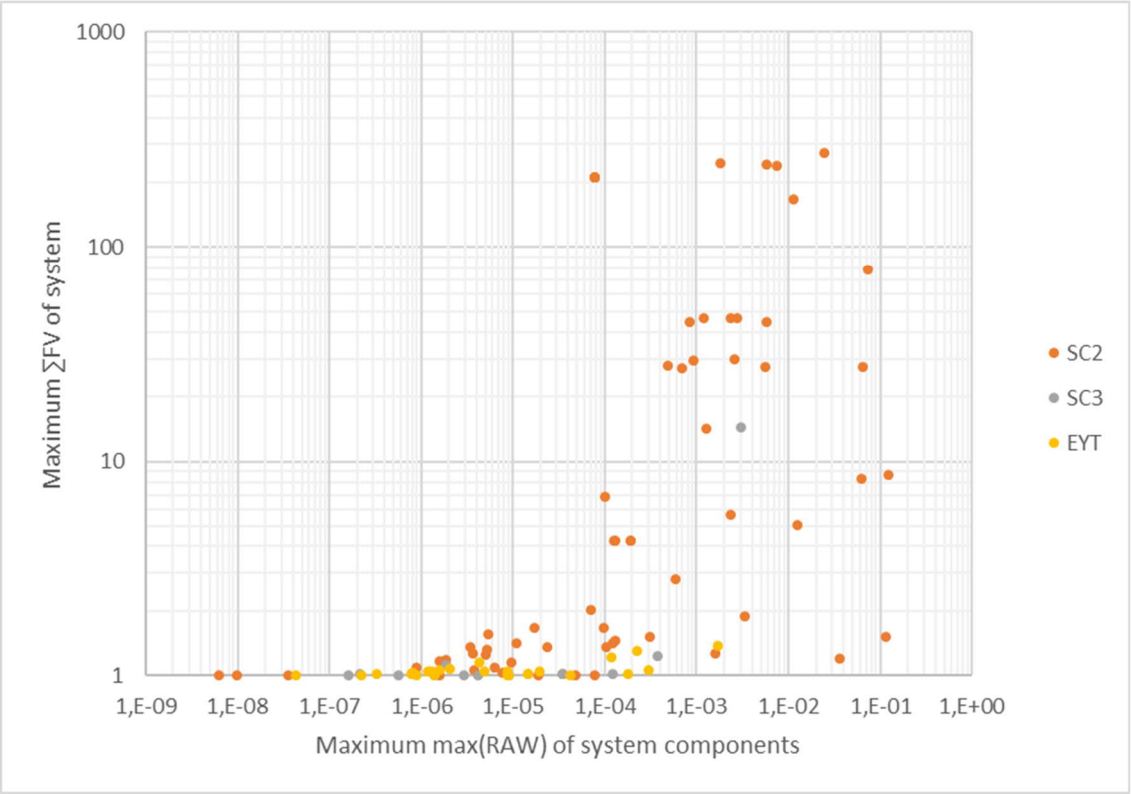


Figure 28 Systems plotted on an FV-RAW plane

5.2 Comparison based on initiating events

5.2.1 Data

The data used in the comparison based on IEs was also obtained from multiple sources:

1. LOMAX [29]: safety classes of components
2. T15X2_19 [45]: IE IDs, descriptions, frequencies
3. Loviisa PRA main report [39] chapter 12 attachments 1 and 2: RIM values of IEs on PRA levels 1 and 2
4. LO1-K854-961-00094 [59] attachments B01-B33: piping segments used in RIISI program and their safety classes

A single IE can be caused by one or multiple different OLs. Some IEs can be considered fault trees of their own where different kinds of combinations of failures can cause the IE. The event itself is still modelled with a single event rather than forming the fault tree within the large fault tree. The event then has only one RIM value, and the different failures are not identified separately. For the RIM values to be comparable to component safety class, the RIM values need to be divided or adjusted according to how the IE is related to failures of different components. Three different ways an IE can be related to a component can be identified:

1. IEs that are a result of a failure of a single component

2. IEs that are a result of failures of multiple components occurring simultaneously due to common or separate causes. This kind of IEs can be considered to consist of one IE and multiple BEs connected to an AND-gate
3. IEs that are a result of a failure of a single component in a group of components. This kind of IEs can be considered to consist of multiple IEs connected to an OR-gate. For example, ITK10Z00FK "TK10-line break outside containment" can be a result of multiple different parts of TK10-line breaking.

For type 1 IEs the CCDP and FV values remain unchanged because they refer only to one component. Type 2 IEs are calculated based on one event identified with frequency and multiple other events identified with probability. For these events, the FV remains constant, but the CCDP value needs to be adjusted according to the probability terms included in the event frequency. The probability terms can be considered to be moved from the term f_{jp} to the term α_{jp} in equation (45). Frequency is divided by the product of the probability terms and term α_{jp} is multiplied by the product.

The frequencies of type 3 IEs are essentially a sum of failure frequencies of multiple components. For this kind of events the CCDP is constant for each component, but the FV value needs to be adjusted according to the frequency that each of the failures contribute to the total IE frequency. Some of the type 3 IEs are calculated as a sum of failure frequencies of individual components. For these IEs, the calculations were used to determine the failure frequency of an individual component and to identify the number of components included in the IE. This enabled to calculate the ratio between frequency contributed by a single component and the total IE frequency. This ratio was then used to calculate the FV of a single component.

Dividing the FV values of some other IEs among the components that can cause the IE is a more complex process. These IEs are not calculated based on the frequencies contributed by individual components. Instead, operating experiences based on larger entities, such as the primary circuit, and from multiple plants are used in order to determine the frequency. Therefore, the calculations of the IE frequencies cannot be used directly to find the share total frequency caused by a single component. Instead the FV value was divided among components with assistance of piping segments that are used for RIISI. When the RIISI-programs were created, the systems within the plant were divided into piping segments and consequences of leakages in each segment were identified with the CCDP value of IEs that the leakage can cause. For this comparison, the segments that each IE can be caused by were identified based on this information and approximate numbers for the amount of component in each segment were calculated. The sum of components from each segment that can cause the IE was used to find the total number of components that can cause the IE. The FV per component was calculated as

$$FV\ per\ component = \frac{FV\ of\ an\ IE}{number\ of\ components\ that\ can\ cause\ the\ IE} \tag{55}$$

The data about IEs was then used to form an array that consists of component level FV and CCDP values and safety classes of all components that can cause IEs. If it was identified that a component or components from a RIISI segment can cause multiple different IEs, the CCDP value was selected as the maximum of the CCDP values and the FV values of the different IEs were added up.

5.2.2 Comparison

In this section, the safety classes of components that can cause IEs are compared to the component level RIM values of the IEs they can cause. There are multiple IEs that can be caused by multiple different components and the components can be from different safety classes. The number of IEs that components from each safety class can cause, and the total number of components that can cause those IEs are shown in Table 6.

Table 6 Number of components included in the comparison from each safety class

Safety class	Number of IEs that components can cause	Number of components that can cause IEs
SC1	15	277
SC2	75	1029
SC3	21	358
EYT	27	395

The components that can cause IEs are plotted on an FV-CCDP plane in Figure 29. Some IEs can be caused by components from multiple safety classes and all the components therefore have the same FV and CCDP values. The safety classes may then overlap each other at multiple points and the FV-CCDP planes have shown separately for each safety class in Appendix 2. It needs to be noted that the points on the plane can also consist of multiple components from the safety class which is not visible when the classes are shown on separate planes either.

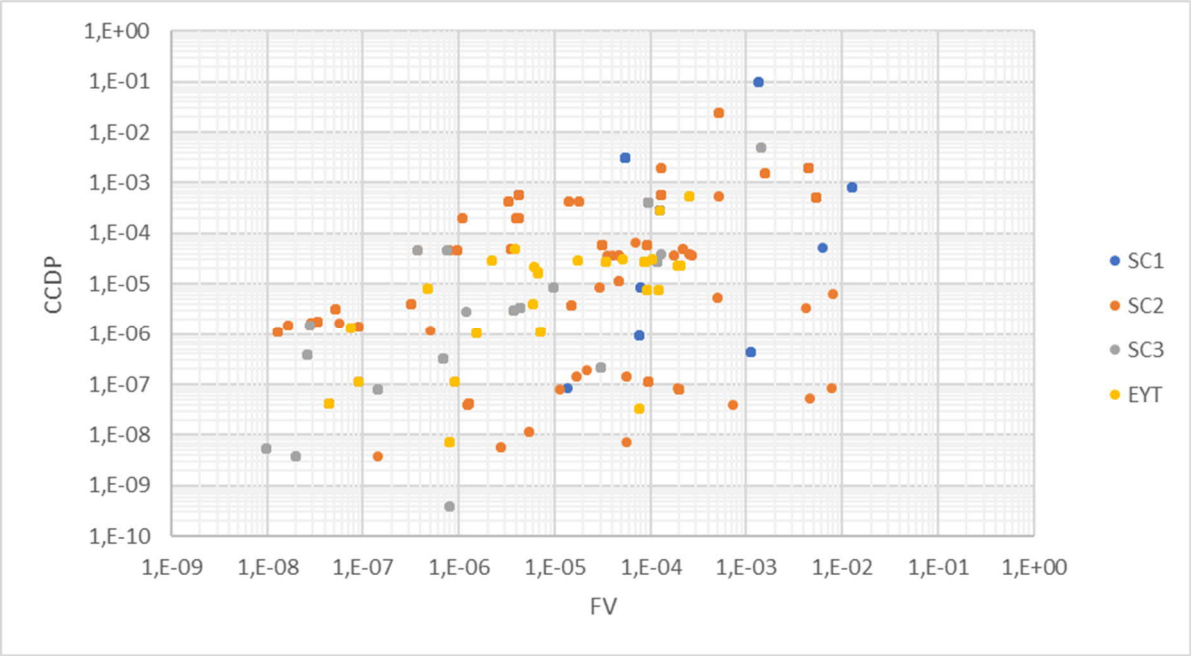


Figure 29 Components on an FV-CCDP plane

It can be seen from the FV-CCDP planes that the RIM values are not completely in line with the safety classes when considering the IEs the components can cause either. Multiple components from the higher safety classes can cause IEs whose RIM values are lower than the RIM values of IEs that components from lower classes can cause.

The SC3 and EYT components have very similar RIM values based on the IEs they can cause. The FV and CCDP values of components from both classes are below the value of 10^{-4} for the most part. CCDP limit of 10^{-4} is actually also used as the limit for identifying piping segments whose leakages have high consequences in the RIISI program [59]. There are some SC3 and EYT components whose RIM values exceed this limit. Some components in class EYT belong to piping segments whose leakages can cause very small leakages outside the containment buildings or very small LOCAs. The CCDP of these IEs exceeds 10^{-4}. The number SC3 components that can cause IEs whose CCDP exceed 10^{-4} is slightly larger but they can also cause few different IEs: steam leakages from steam generator blow-down lines and a small or very small LOCAs.

The highest ranking SC1 and SC2 components also can have very similar CCDP and FV values, but highest values are those of SC1 components. On average the SC1 components still have higher RIM values than the SC2 components. This is shown by values collected in Table 7. This is similar to how the BE RIMs were found to related to the safety class. However, the FV values of EYT components in the model seem to be higher on average than the FV values of SC3 components. But for example, the number of SC3 components that exceed the $CCDP = 10^{-4}$ limit is higher than the number of similar EYT components.

Table 7 Measures of middle and spread calculated for IE RIMs when all components that can cause Ies are included

CCDP				
Safety class	**Max**	**Average**	**Median**	**90th percentile**
SC1	1,0E-01	3,1E-03	5,7E-04	1,9E-03
SC2	2,4E-02	6,0E-04	2,9E-04	5,7E-04
SC3	5,1E-03	1,5E-04	3,3E-06	3,9E-04
EYT	5,3E-04	2,8E-05	7,9E-06	3,0E-05
ALL	1,0E-01	7,5E-04	6,0E-05	5,7E-04
FV				
Safety class	**Max**	**Average**	**Median**	**90th percentile**
SC1	1,3E-02	2,1E-03	1,3E-04	5,5E-03
SC2	8,0E-03	7,6E-04	9,6E-05	4,4E-03
SC3	1,4E-03	5,5E-05	4,4E-06	1,3E-04
EYT	2,6E-04	6,3E-05	3,5E-05	1,9E-04
ALL	1,3E-02	7,0E-04	8,8E-05	4,4E-03

Distributions of the component FV and CCDP values calculated based on IEs are shown in Figures 30 and 31. It can be seen from the figures also that the CCDP values are more in line with the safety classes of components. The distribution of EYT components is slightly above the distribution of SC3 components at the lower CCDP values, but there is still more SC3 components that have higher CCDP values. The distributions of FV values are almost identical for SC3 and EYT components that can cause IEs.

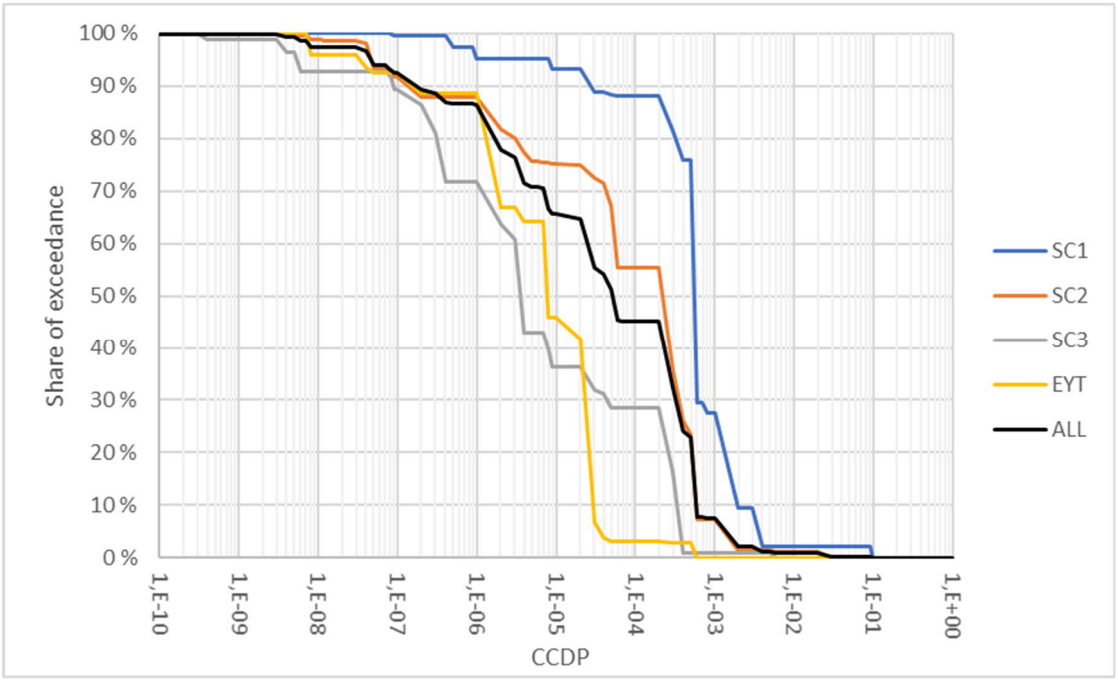


Figure 30 Distributions of CCDP values of components

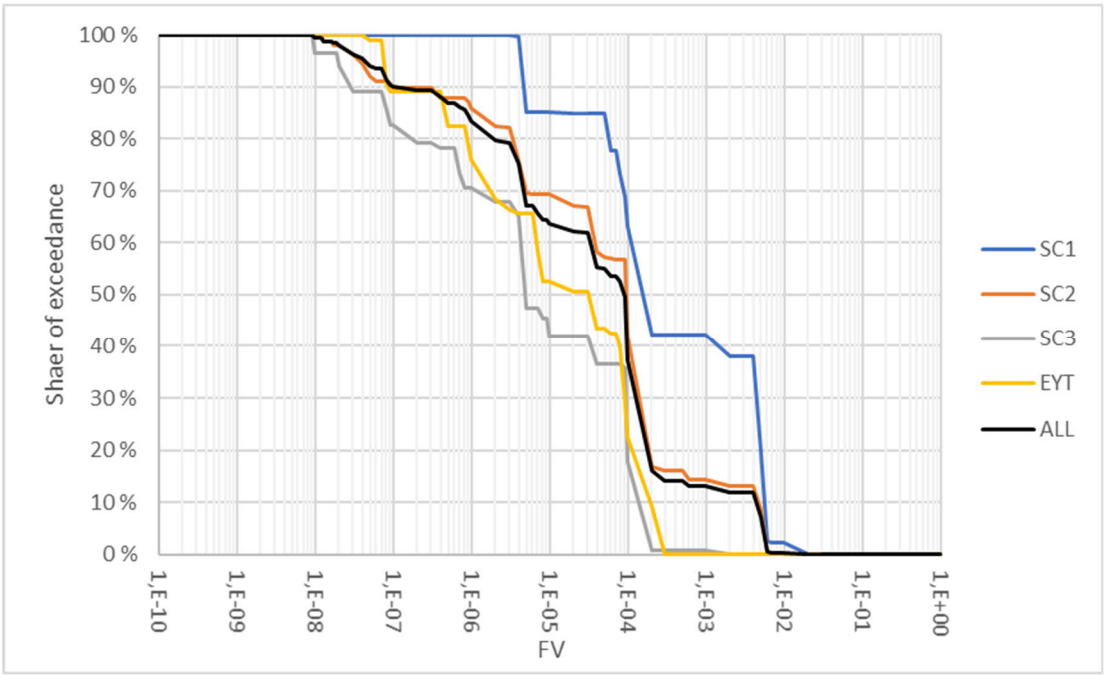


Figure 31 Distributions of FV values of components calculated based on IEs

Some components were most likely included twice in the comparison because the exact KZ-IDs were not identified. There may also have been some deviations between the actual numbers of components in the RIISI segments and the number that was used in this thesis. This may have caused some deviations in the FV-values of components. The pipes between the components were also ignored which may overestimate the FV values of the IEs some components can cause. Assuming for example that 30% of every leakage IE frequency is a result of pipe ruptures would result in the FV values of individual components being decreased by the same amount. The CCDP values of individual components are not affected by the possible errors in calculation of total number of components and by the ignoring of

pipe ruptures. Therefore, the CCDP values should be more accurate. It could also have been possible to identify the exact OLs that can cause each IE, but considering the numbers in Table 6 it would have been a very time consuming task and the changes to the results may not have been that large.

Some differences can be noticed when the distributions created based on IE RIMs are compared to the ones created based on BE RIMs. The distributions of FV values calculated for all components modelled with BEs and IEs are compared to each other in Figure 32. Similar figures for all safety classes separately are provided in Appendix 3. Some differences between the distributions are guaranteed to exist due to the modelling with BEs being based on specific failure modes of individual components rather than using one BE to model multiple components. Due to multiple components in each safety class sharing the same RIM values the distributions are also a lot rougher. The differences between the number of high FV components are the biggest for SC2 components. For components in all safety classes the highest-ranking components seem to have higher FV values based on BEs than based on IEs. This is probably because important components can be used in response to multiple different IEs in multiple accident sequences, while the IEs only belong to one accident sequences. However, the IEs also belong to all MCSs that are solved based on one accident sequence and therefore the FV value can in some cases be higher when calculated based on IEs.

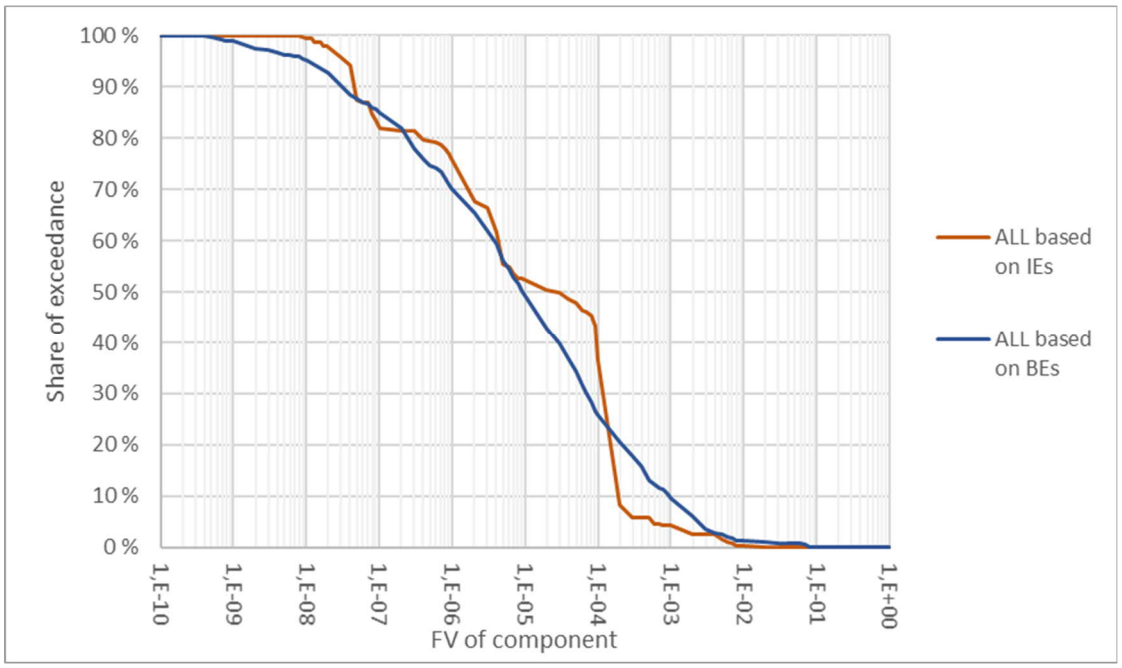


Figure 32 Distributions of component-level FV values calculated for all components modelled with BEs and for all components modelled with IEs

5.3 Suggestion for guiding values

Based on the comparisons previous two sections it can be concluded that every safety class has components that can be considered more significant than some components in a higher safety class. The RIM values of components in each safety class cover a wide range of different RIM values with the lower limit for the range for each class being very close to the minimum value possible for the RIM in consideration. However, the upper limit varies depending on the safety class. These upper limits can be used to identify how large RIM

values can components in each class currently have. These upper limits can then be used when considering the classification of components in a new system, or reclassification of existing components. If there are currently no EYT components with very high RIM values, it would not be sensible to classify a new component with a very high RIM value into that class.

Upper limits are also used in the American guidelines to determine whether or not a component can be considered non-safety significant according to the RIM values [68]. Following how the limits divide the FV-RAW plane into two sectors in [68], the FV-RAW and FV-CCDP planes can be divided analogously into sectors for each safety classes as illustrated in Figure 33. The upper limits for safety classes should be set based on both BEs and IEs. If any of the upper limits set for a safety class is exceeded, then the component should be placed into a higher safety class according PRA. Also, the RIM values of other components that the component needs to share the class with should be taken into account. Such limits could primarily be used to give indication whether there is a need from PRA perspective to safety classify the component. Undercutting all EYT upper limits would not directly mean that a component should be classified as EYT, but that it can be classified as EYT from PRA perspective. If a component should be classified to a different safety class according to BEs and IEs, the higher safety class should be used analogously to selecting the higher safety class from the functional and structural safety classes.

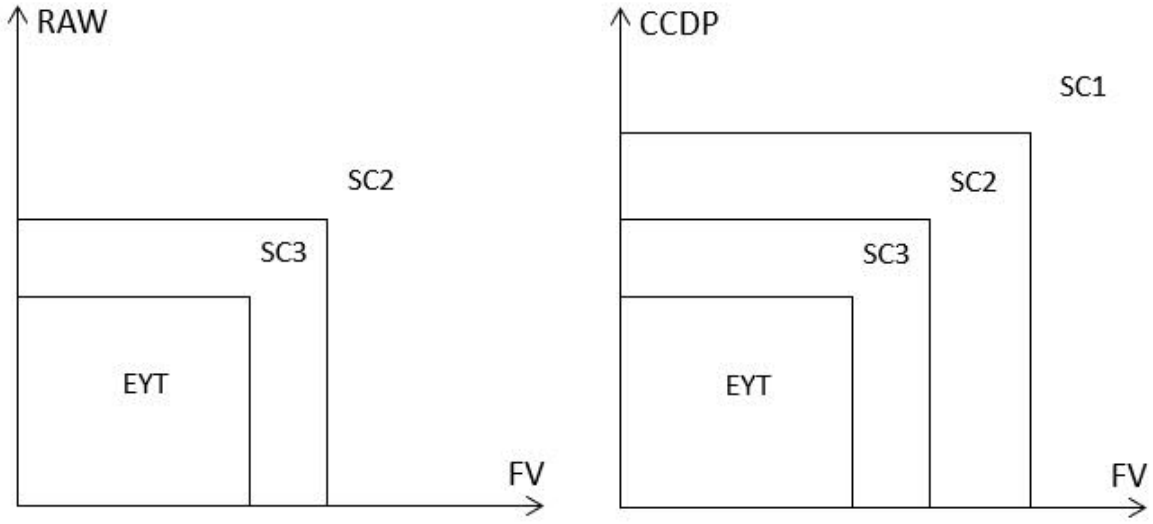


Figure 33 FV-RAW and FV-CCDP planes divided into sectors

The highest safety class is SC2 in the FV-RAW plane because it was found that multiple SC2 components rank higher than SC1 components based on the BE RIMs. SC2 is also the highest safety class for automation- and electrical systems and therefore even if an electrical component exceeds the IE RIM limits for SC2, it should still be classified as SC2.

Multiple different methods of determining component level RAW were used in Section 5.1. The RAW values can be selected as maximums of individual failure RAWs and CCF RAWs separately, or with the weighted average method. Therefore, there are two different combinations of RIMs that can be used to measure component risk and safety significance based on BEs:

1. $K_k^{RAW,single}$, $K_k^{RAW,all}$ and K_k^{FV}
2. $K_k^{RAW,wam}$ and K_k^{FV}

In order to find out which combination of RIMs matches the current classification better, two questions can be asked about the suggested limits on BE RIM values to test how well they match the current safety classification

1. If components were reclassified strictly based on the suggested limits, how large share of components in a safety class would keep their safety class?
2. If components were reclassified strictly based on the suggested limits, how much would the number of components within a safety class change?

The upper limits for safety classes SC3 and EYT were selected based on the 90th percentiles calculated for component groups. Maximum values are very absolute, but percentiles give some tolerance for anomalies within each safety class. Using the 90th percentile ignores the top 10% most important component groups in both safety classes thus giving some tolerance against the anomalies. The components in the same group were also assumed to be reclassified into the same new group.

Percentages that show the answers to the two questions above are collected in Table 8 below. These were calculated by comparing the RIM values of each component to the suggested limits. Components from SC1 were not assumed to be reclassified in the calculations. It can be seen that both methods to calculate component RIM match the current classification quite well. More components would keep their current safety class if the RAW was calculated as maximums. Also the total number of components in SC2 and SC3 would decrease less.

Table 8 Upper limits based on BEs tested against current classification

When upper limits are selected based on the 90th percentiles of ∑FV, max(RAW,single) and max(RAW,all) of component groups					
Safety class	**∑FV limit**	**max(RAW, single) limit**	**max(RAW,all) limit**	**Share of components that would keep the same SC**	**New count / old count of components**
SC2	-	-	-	57 %	79 %
SC3	8,51E-04	1,30	3,19	21 %	55 %
EYT	5,93E-05	1,15	1,21	77 %	248 %

When upper limits are selected based on the 90th percentiles of ∑FV and RAW,wam of component groups				
Safety class	**∑FV limit**	**RAW,wam limit**	**Share of components that would keep the same SC**	**New count / old count of components**
SC2	-	-	45 %	64 %
SC3	8,51E-04	1,41	24 %	69 %
EYT	5,93E-05	1,17	82 %	266 %

The upper limits for IE RIM values can be determined similarly, but an upper limit can also be determined for SC2. It would probably be very difficult to reason for reduction of the

safety class of an SC1 component and increasing the safety class of an SC2 component to SC1 would not probably be worth the increased safety it possibly achieves. The PRA results are already considered in the RIISI programs and the RIM values are taken into account. Therefore, there should be a very strong basis to consider reclassifying an SC2 component as SC1 instead and the SC2 upper limit for FV and CCDP values is suggested based on the maximum of the FV and CCDP values of SC2 components. The component FV values calculated from IE RIMs are very subject to errors in the calculation of total number of components per RIISI segment. Therefore, the FV upper limits for IEs should be probably be selected to match the FV limits calculated based on BEs. The suggested upper limits for IEs and percentages showing how well they match the current classification are shown in Table 9 below. SC1 was also ignored from these calculations.

Table 9 Upper limits based on IEs tested against the current classification

Safety class	FV limit	CCDP limit	Share of components that would keep the same SC	New count / old count of components
SC2	7,97E-03	2,37E-02	36 %	43 %
SC3	8,51E-04	3,94E-04	23 %	208 %
EYT	5,93E-05	2,99E-05	52 %	158 %

The suggested upper limits for each safety class based on BEs and IEs are all rounded and collected in Table 10.

Table 10 Suggested guiding limits for use in assistance of safety classification

	Basic events			Initiating events	
Safety class	**∑FV**	**max(RAW,single)**	**max(RAW,all)**	**FV**	**CCDP**
SC2	-	-	-	1E-01	1E-02
SC3	1E-03	1,3	3,2	1E-03	5E-04
EYT	5E-05	1,1	1,2	5E-05	5E-05

If the level 2 RIM values were used instead and the upper limits were selected similarly, the resulting upper limits would be the limits shown in Table 11. The RIMs whose value is relative to the top event frequency would stay similar to the limits on level 1, but the CLRP values would change by different factors. The top event frequency on level 2 is about half of the top event frequency on level 1 which causes the differences. The changes are biggest for SC2 for which the CLRP limit is only a tenth of the limit for CCDP values.

Table 11 Suggested guiding limits when RIM values from level 2 are used

	Basic events			Initiating events	
Safety class	**∑FV**	**max(RAW,single)**	**max(RAW,all)**	**FV**	**CLRP**
SC2	-	-	-	1E-01	1E-03
SC3	1E-03	1,2	2,7	1E-03	1E-04
EYT	1E-04	1,1	1,2	1E-04	1E-05

5.4 Discussion

There are multiple sources of error that affect the guiding limits defined in the previous section. The PRA models themselves are not perfect representations of the actual NPP. The models do not include every SSC and every relationship between the SSCs. It is possible that all relevant accident sequences have yet not been identified. There are also multiple assumptions made about how one event would lead to another, and multiple simplifications in the calculation of event parameters. One example of a simplification used in Loviisa PRA model is that some components in altering operation are assumed for modelling purposes to be operated in such a way that one component is always in standby and the other is always operating. The assumptions made in the calculation of different parameters are usually conservative, but when considering the categorization, the different levels of conservativity affect the relative rankings.

The upper limits for RIM values were determined separately for each RIM. This ignores the possibility that a component can be very significant according to both FV and RAW, but the value of neither exceeds the upper limits set for a safety class. Such a component can be actually more significant than a component that is significant only according to one RIM, but not the other. Therefore, attention should also be paid to components whose RIM values are both close to the determined guiding limits. Some components can have an important role in prevention of IEs from propagating into accidents while their failures can also cause IEs with significant consequences. Combining the FV values of the BEs and IEs modelling the component would increase the total FV values. This possibility was ignored from the comparisons due to the BEs and IEs being handled separately and also because the IEs were not associated with the exact KZ-IDs.

If a component is considered important according to the RIM values, changing the safety class is not the only option to increase the safety of the plant. Depending on the RIM that is considered high for the component, other adjustive measures could be taken. If the RAW or CCDP values are high, then plant modifications could be added to increase the defence-in-depth against failures of that individual component. If FV is high, then measures could be taken to decrease the unavailability or failure rate of the component. For example, the maintenance programs, inspections or allowed repair times can be adjusted according to the component importance. Attention should also be paid to what kind of failures can cause the component RIM values to exceed the limits and how much changing the safety class can affect those failures. For example, if plant data is used for a component and none of the previous failures are mechanical ones, it may not actually be sensible to increase the mechanical safety class based on the data.

6 Conclusions

The safety classes of SSCs and the RIMs that can be calculated for SSCs with PRA models both measure the importance of an SSC. In this thesis the main objectives were to compare the current safety classes of SSCs in a Finnish NPP to the RIM values of the same SSCs, and to determine guiding values that can be used in assistance when new SSCs are added to the plant and when the current SSCs are considered to be reclassified. A secondary objective was to study the RIMs that can be currently calculated with RiskSpectrum PSA 1.3.2 or from the calculated results and how they are currently used in safety classification.

Background information on nuclear power and nuclear safety were provided first and then the safety classification in Finland was described. Then, the PRA methodology was introduced with focus on the contents and quantification of a PRA model in order to provide the necessary information required for understanding what the different RIMs measure and how they are calculated. The different RIMs that can be calculated for BEs and IEs with RiskSpectrum PSA 1.3.2 and the calculation and interpretation of the RIM values were then introduced. It was found that all of the RIMs depend on the system configuration of the plant, while some of them also depend on the probability or frequency of the event. Then, the applications of RIMs to measure the importance of a whole component, or system or safety function were discussed. The effect that the safety class has on the current RIM values was also discussed, but it was concluded that there are multiple factors that affect the RIM values and the direct dependence on safety class could not be identified.

Three RIMs were selected for the comparison: FV, RAW and CCDP. FV measures the probability that the top was caused by an MCS that contains the component and the share of top event frequency that is caused by MCSs that contains the component. RAW measures the consequences of component unavailability as an increase in the top event frequency. CCDP measures the conditional probability of top event given that the component causes an IE. The comparisons were carried out for RIMs calculated for BEs and IEs separately. Structures are generally not classified in Loviisa NPP. Therefore, the comparisons primarily included components. A large share of internal IEs was found out to be used to model larger entities than a single components. CCDP values were found to be equal for all the components that can cause the same IE, but FV values had to be divided for the components. In order to find out the approximate numbers of components that can cause the IE, and their safety classes, the piping segments identified for RIISI were used in assistance. More accurate comparisons based on IE RIMs could be carried out if it was better determined which components can cause each IE and what is their actual share of the IE frequency.

The comparisons between safety classification and RIM values of components were carried out by analyzing the components on different types of plots, through relative rankings and based on the absolute values of the RIMs. It was found that safety classes are not completely in line with the RIM values. For example, there are multiple EYT components whose RIM values exceed the RIM values of SC2 components. This shows that there would be a lot of opportunities to optimize the safety classes. However, the components from a high safety class tend to have higher RIM values on average than components from the lower safety classes. It was also found that SC1 are not more important than SC2 components according to the RIMs calculated for BEs. The SC1 components are still more significant than SC2 components when analyzing IEs which are more related to structural failures. While each safety class was found to contain components whose RIM values are close to the minimum

value of the RIM, the maximums were found to be higher for higher safety classes for the most part.

A suggestion for guiding values to be used in safety classification in order to comply with the requirement set in YVL B.2 was then presented and tested against the current classification. The guiding values were suggested to be used as upper limits for each safety class. If the RIM value of the component or any component that the component has to have the same safety class with exceeds the upper limit, then the component should be classified to the above class. The upper limits were determined based on what kind of RIM values the components currently in each class can have. They were tested against the current safety classes of components by analyzing how the safety classes of components would change if all components were classified based only on the RIM values. The suggested limits should be used to give indication whether or not there is need from PRA perspective to safety classify a component or to have the component in a higher safety class. PRA should not be used as the only means to justify reducing the safety class of a component if the component is required to be in a specific class according to YVL B.2 guidelines. PRA could also be used to find components that could be candidates for reduction of the safety class, but every case should be analyzed separately.

The suggested values were determined to be used within the current guidelines but depending on the coverage and accuracy future PRA models, the safety classification in Finland could be moved to be more based on the PRA. In an optimum situation the SSCs with the highest RIM values would also be the ones in the highest safety classes. Or in order to take the deterministic analyses also into account, something similar to the American risk-informed safety categorization could be implemented where less significant safety classified components would be subject to some easements regarding the requirements and more significant EYT SSCs would have their requirements increased.

References

[1] International Atom Energy Agency. *Preliminary Nuclear Power Facts and Figures for 2019*. Available: https://www.iaea.org/newscenter/news/preliminary-nuclear-power-facts-and-figures-for-2019 [revised 13.4.2020].

[2] Statistics Finland. *Energia – Energian kokonaiskulutus*. Available: https://www.stat.fi/tup/suoluk/suoluk_energia.html [revised 13.4.2020].

[3] Radiation and Nuclear Safety Authority. *Regulatory Guide on nuclear safety YVL B.2, Classification of systems, structures and components of a nuclear facility*. Available: http://www.finlex.fi/data/normit/41768-YVL_B.2e.pdf [revised 13.4.2020]

[4] Männistö, I. *Risk-Informed Classification of Systems, Structures and Components in Nuclear Power Plants*. Master's thesis. Helsinki University of Technology, Department of Engineering Mathematics and Physics. Espoo, 2005. 75 p.

[5] Julin, A. *Use of probabilistic safety assessment in supporting regulatory authority's work*. STUK-YTO-TR 94. Helsinki, 1995. 63 p. Available: https://inis.iaea.org/collection/NCLCollectionStore/_Public/27/041/27041685.pdf [revised 13.4.2020]

[6] Fortum Power and Heat. *Loviisan ydinvoimalaitos*. Available: https://www.fortum.fi/tietoa-meista/yhtiomme/energiantuotantomme/voimalaitoksemme/loviisan-ydinvoimalaitos [revised 13.4.2020]

[7] Sandberg, J. *Ydinturvallisuus*. Helsinki: Säteilyturvakeskus, 2004. 481 p. ISBN 951-712-507-0 (electronic).

[8] Fortum Power and Heat. *Loviisa Nuclear Power Plant – Operations*. Available: https://www.fortum.com/about-us/our-company/our-energy-production/our-power-plants/loviisa-nuclear-power-plant/operations [revised 13.4.2020]

[9] American Nuclear Society, Nuclear Facility Standards Committee. *Glossary of definitions and terminology*. 2009. Available: http://www2.ans.org/standards/resources/toolkit/docs/nfsc-glossary-9-2009.pdf [revised 13.4.2020]

[10] Murray, R. Holbert, K. *Nuclear Energy - An Introduction to the Concepts, Systems, and Applications of Nuclear Processes*. 7th Edition. Amsterdam: Elsevier, 2015. ISBN 978-0-12-416636-3 (electronic).

[11] Kotola, R. Pirinen, H. *Final Safety Assessment Report chapter 1.2 Laitoksen yleiskuvaus*. Internal document. Fortum Power and Heat, 2018.

[12] Petrangeli, G. *Nuclear Safety*. 1st edition. Amsterdam: Butterworth-Heinemann, 2006. 429p. ISBN 978-0-7506-6723-4.

[13] The American Society of Mechanical Engineers. *Standard for probabilistic risk assessment for nuclear power plant applications*. 2000. Available: https://www.nrc.gov/docs/ML0037/ML003733342.pdf [revised 13.4.2020]

[14] *Nuclear Energy Act 1988/161*. Available: https://www.finlex.fi/fi/laki/ajantasa/1988/19880161 [revised 13.4.2020]

[15] Radiation and Nuclear Safety Authority. *Regulatory Guide on nuclear safety YVL B.1, Safety design of a nuclear power plant*. Available: https://www.stuklex.fi/en/ohje/YVLB-1 [revised 13.4.2020]

[16] Ahokas, J. *Final Safety Assessment Report chapter 3.6 Järjestelmien toiminnalliset perusteet*. Internal document. Fortum Power and Heat, 2018.

[17] Fortum Power and Heat. *Ydinturvallisuus Loviisan voimalaitoksella*. Available: https://www.fortum.fi/tietoa-meista/yhtiomme/energiantuotantomme/voimalaitoksemme/loviisan-voimalaitos/ydinturvallisuus-loviisan-voimalaitoksella [referred 15.4.2020]

[19] International Atom Energy Agency. *Specific Safety Guide SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants*. 2014. Available: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1639_web.pdf [revised 13.4.2020]

[20] Piensalo, J. *Final Safety Assessment Report chapter 8.1 Sähköjärjestelmät - johdanto. Internal document*. Fortum Power and Heat, 2017.

[21] Suontama, H-L. *Final Safety Assessment Report chapter 3.8 Automaatio- ja valvomoarkkitehtuurit*. Internal document. Fortum Power and Heat, 2019.

[22] Kelavirta, T. T-01-00015, *KZ-tunnusten määrittely, varaus ja tunnisteiden tilaaminen*. Internal document. Fortum Power and Heat, 2017.

[23] *Nuclear Energy Act 1987/990*. Available: https://www.finlex.fi/fi/laki/ajantasa/1987/19870990 [revised 13.4.2020]

[24] Radiation and Nuclear Safety Authority. *Regulatory Guide on nuclear safety YVL A.7, Probabilistic risk assessment and risk management of a nuclear power plant*. Available: https://www.stuklex.fi/en/ohje/YVLA-7 [revised 13.4.2020]

[25] International Atom Energy Agency. *Specific Safety Requirements No. SSR-2/1, Safety of Nuclear Power Plants: Design*. Vienna, 2016. Available: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf [revised 13.4.2020]

[26] Radiation and Nuclear Safety Authority. *Regulatory Guide on nuclear safety YVL B.2, Classification of systems, structures and components of a nuclear facility, Explanatory memorandum*. Available: https://www.stuklex.fi/en/STUK-Y-1-2018_perust.pdf [revised 13.4.2020]

[27] Wahlström, B. Sairanen, R. *Views on Finnish nuclear regulatory guides*. Säteilyturvakeskus, 2011.

[28] Kelavirta, T. *MO-05-00030, Turvallisuus- ja maanjäristysluokitusasiakirjojen sekä PI-kaavioiden ylläpito*. Internal document. Fortum Power and Heat, 2019.

[29] *LOMAX Asset Management System*

[30] Ahokas, J. Suurnäkki, O. *Final Safety Assessment Report chapter 3.2 Järjestelmien, rakenteiden ja laitteiden luokitus*. Internal document. Fortum Power and Heat, 2018.

[31] Bedford, T. Cooke, R. *Probabilistic Risk Analysis: Foundations and Methods*. 1st ed. New York: Gambridge University Press, 2011. 414 p. ISBN 978-0-521-77320-1.

[32] Leino, K. *MO-05-00019, Loviisan todennäköisyyspohjaisen riskianalyysin (PRA) ylläpito ja soveltaminen*. Internal document. Fortum Power and Heat, 2018.

[33] Rasmussen, N. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. U.S. Nuclear Regulatory Commission, 1975.

[34] Keller, W. Modarres, M. *A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor Norman Carl Rasmussen*. Reliability Engineering & System Safety [online journal]. Vol 89: 3. 2005. P 271-285. [revised 13.4.2020]. Available: https://doi.org/10.1016/j.ress.2004.08.022

[35] Hickman, J. et al. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants: Chapters 1–8 (NUREG/CR-2300, Volume 1)*. U.S. Nuclear Regulatory Commission, 1983. Available: https://www.nrc.gov/docs/ML0635/ML063560439.pdf [revised 13.4.2020]

[36] Fortum Power and Heat. *Loviisa 1 Turvallisuustekniset käyttöehdot*. Internal Document. 2020.

[37] Himanen, R. Julin, A. Jänkälä, K. Holmberg, J-E. Virolainen, R. *Risk-Informed Regulation and Safety Management of Nuclear Power Plants – On the Prevention of Severe Accidents*. Risk Analysis [online journal]. Vol 32: 11. 2012. P. 1978-1993. Available: DOI: 10.1111/j.1539-6924.2012.01904.x [revised 13.4.2020]

[38] Reliability Education. *Reliability Prediction Basics*. 2007. Available: https://www.reliabilityeducation.com/reliabilityeducation/ReliabilityPredictionBasics.pdf [revised 13.4.2020]

[39] Jänkälä, K. Paavola, I. Sirén, S. Pyy, T. Koskenranta, J. Hotakainen, R. *Loviisan ydinvoimalaitoksen riskitutkimus, pääraportti*. Internal document. Fortum Power and Heat Oy, 2019.

[40] Modarres, M. Kaminskiy, M. Krivtsov, V. *Reliability Engineering and Risk Analysis – A Practical Guide*. 3rd edition. CRC Press LLC, 2017. 523 p. ISBN 978-1-49874-587-1.

[41] Vaurio, J. *Luotettavuustekniikka*. Supplementary Material. Lappeenranta University of Technology, Department of Energy- and Environmental Technology, 2007. 159 p.

[42] Lloyd's Register Consulting – Energy AB. *RiskSpectrum Analysis Tools Theory Manual. Version 3.3.0*.

[43] Beeson, S. *Non-Coherent fault tree analysis*. Doctoral Thesis. Loughborough University. Loughborough, 2002. 257 p. Available: https://hdl.handle.net/2134/6927 [revised 13.4.2020]

[44] Fortum Power and Heat. *PSADATA*. Internal Excel-file. 2019.

[45] Fortum Power and Heat. *T15X2_19*. Internal Excel-file. 2019.

[46] Van der Borts, M. Schnoonakker, H. *An overview of PSA importance measures*. Reliability Engineering & System Safety [online journal]. Vol 72: 3. 2001. P. 241-245. Available DOI: 10.1016/S0951-8320(01)00007-2 [revised 13.4.2020].

[47] Meng, F-C. *Relationships of Fussell-Vesely and Birnbaum importance to structural importance in coherent systems*. Reliability Engineering & System Safety [online journal]. Vol 67: 1. 2000. P. 55-60. Available DOI: 10.1016/S0951-8320(99)00043-5 [revised 13.4.2020].

[48] Cross, R. Youngblood, R. *Probabilistic Risk Assessment Procedures Guide for Offshore Applications, Draft*. Technical Report. 2016. Available: https://www.bsee.gov/sites/bsee.gov/files/ProbalisticRiskAssessment%20%28PRA%29/bsee_pra_procedures_guide_-_10-26-17.pdf [revised 13.4.2020]

[49] Vrbanic, R. Samanta, P. *Risk Importance Measures in the Design and Operation of Nuclear Power Plants*. New York: The American Society of Mechanical Engineers, 2017. 141 p. Available: https://www.bnl.gov/isd/documents/95367.pdf [revised 13.4.2020]

[50] Martonell, S. Serradell, V. Verdú, G. *Safety-related equipment prioritization for reliability centered maintenance purposes based on plant specific level 1 PSA*. Reliability Engineering & System Safety [online journal]. Vol 52: 1. 1996. P. 35-44. Available DOI: 10.1016/0951-8320(95)00122-0 [revised 13.4.2020].

[51] Jänkälä, K. *A risk informed safety classification for a Nordic NPP*. Nordic Nuclear Safety Research. Report NKS-72. Roskilde: NKS Secretariat, 2002. ISBN 87-7893-128-2. Available: https://inis.iaea.org/collection/NCLCollectionStore/_Public/33/055/33055512.pdf [revised 13.4.2020]

[52] Cheok, M. Parry, G. Sherry, R. *Use of importance measures in risk-informed regulatory applications*. Reliability Engineering & System Safety [online journal]. Vol 60: 3. 1998. P. 213-226. Available DOI: 10.1016/S0951-8320(97)00144-0 [revised 13.4.2020].

[53] Vaurio, J. *Developments in importance measures for risk-informed ranking and other applications*. Proceedings of PSAM 8 conference in New Orleans, 14–19. New York: ASME, 2006.

[54] Birnbaum, Z. *On the Importance of Different Components in a Multicomponent System*. Technical Report No. 54. University Of Washington, Department of Mathematics. Seattle, Washington. 1968. Available: https://apps.dtic.mil/sti/pdfs/AD0670563.pdf [revised 13.4.2020].

[55] Wall, I. Haugh, J. Worlege, D. *Recent applications of PSA for managing nuclear power plant safety*. Progress in Nuclear Energy [online journal]. Vol 39: 3-4. 2001. P. 367-425. Available DOI: 10.1016/S0149-1970(01)00021-X [revised 13.4.2020]

[56] Borgonovo, E. *Differential, criticality and Birnbaum importance measures: An application to basic event, groups and SSCs in event trees and binary decision diagrams*. Reliability Engineering & System Safety [online journal]. Vol 92: 10. 2007. P. 1458-1467. Available DOI: 10.1016/j.ress.2006.09.023 [revised 13.4.2020]

[57] Borgonovo, E. Apostolakis, G.E. *A new importance measure for risk-informed decision making*. Reliability Engineering & System Safety [online journal]. Vol 72: 2. 2001. P 193-212. Available DOI: 10.1016/S0951-8320(00)00108-3 [revised 13.4.2020]

[58] Vaurio, J. *Ideas and developments in importance measures and fault-tree techniques for reliability and risk analysis*. Reliability Engineering & System Safety [online journal]. Vol 95: 2. 2010. P. 99-107. Available DOI: 10.1016/j.ress.2009.08.006 [revised 13.4.2020]

[59] Fortum Power and Heat. *LO1-K854-961-00094 LO1 putkistojen riskiperustainen määräaikaistarkastusohjelma 10 -vuotisjaksolle 2018-2027*. Internal Document. 2018.

[60] Kim, K. Kang, D. Yang, J. *On the use of the Balancing Method for calculating component RAW involving CCFs in SSC categorization*. Reliability Engineering & System Safety [online journal]. Vol 87: 2. 2005. P. 233-242. Available DOI: 10.1016/j.ress.2004.04.017 [revised 13.4.2020]

[61] Vaurio, J. *Importance measures in risk-informed decision making: Ranking, optimisation and configuration control*. Reliability Engineering & System Safety [online journal]. Vol 96: 11. 2011. P. 1426-1436. Available DOI: 10.1016/j.ress.2011.06.012 [revised 13.4.2020]

[62] U.S. Nuclear Regulatory Commission. *Regulatory Guide 1.174, An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis*. Revision 3. 2018. Available: https://www.nrc.gov/docs/ML1731/ML17317A256.pdf [revised 13.4.2020]

[63] Ahokas, J. Brunner, E. *LO1-K604-604-00029 Automaatiotekninen turvallisuusluokitusasiakirja*. Internal document. Fortum Power and Heat Oy, 2019.

[64] Radiation and Nuclear Safety Authority. *Regulatory Guides on Structures and equipment of a nuclear facility*. Available: https://www.stuklex.fi/en/yvl-ohje [revised 13.4.2020]

[65] Raitanen, O. *Use of Commercial-Grade Items in Nuclear Facilities*. Master's Thesis. Tampere University of Technology. Tampere, 2017. 93 p.

[66] Ahokas, J. *LO1-K8048-00018 PSR2019, Loviisan voimalaitoksen turvallisuusluokituserot verrattuna ohjeen YVL B.2 vaatimuksiin*. Internal Document. Fortum Power and Heat Oy, 2018.

[67] U.S. Nuclear Regulatory Commission. *§ 50.69 Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors*. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0069.html [revised 13.4.2020]

[68] U.S. Nuclear Energy Institute. *10 CFR 50.69 SSC Categorization Guideline*. Revision 0. 2005. Available: https://www.nrc.gov/docs/ML0529/ML052910035.pdf [revised 13.4.2020]

[69] Mandelli, D. Parisi, C. Ma, Z. Maljovec, D. Alfonsi, A. Smith, C. *Light Water Reactor Sustainability Program, Risk-Informed Analysis of Commercial Nuclear Reactors: the RISMC Approach and 10CFR50.69*. Idaho National Laboratory,

2017. Available:
https://pdfs.semanticscholar.org/4416/3e37fee8d056089a6657f60f28c6017ab8d4.pdf [revised 13.4.2020]

[70] Jun, Z. Jiejuan, T. Xuhong, H. *Risk-informed categorization of the SSCs in NPPs*. 18th International Conference on Structural Mechanics in Reactor Technology (SMiRT 18). Beijing, China, 2005. Available: https://repository.lib.ncsu.edu/bitstream/handle/1840.20/31812/O01_10.pdf [revised 13.4.2020].

[71] Holmberg, J.E. Pulkkinen, U. Rosqvist, T. Simola, K. *Decision criteria in PSA applications (NKS-44)*. Roskilde: Nordic nuclear safety research, 2001. ISBN 87-7893-097-9. Available: https://inis.iaea.org/collection/NCLCollectionStore/_Public/33/036/33036832.pdf [revised 13.4.2020]

[72] Fortum Power and Heat. *LO1-K504-504-00004 Sähköjärjestelmien ja -laitteiden turvallisuusluokitus*. Internal Document. 2020.

List of appendices

Appendix 1. Criteria used to measure risk and safety significance in literature

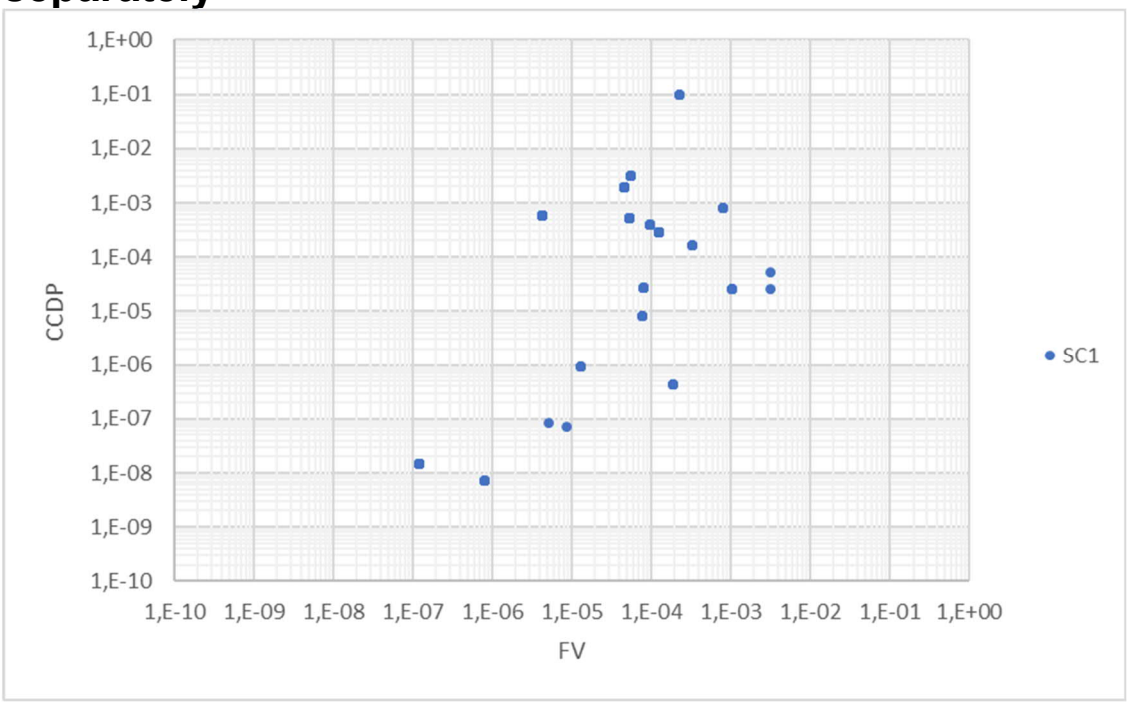
Appendix 1 – Table 1 Criteria used to measure component significance collected in [71]

Decision case	Criteria	Acceptance or criticality values
Consequence assessment of assumed initiating event	CCDP	>1E-4 high 1E-6…1E-4 medium <1E-6 low
	CLERP	>1E-5 high 1E-7…1E-5 medium <1E-7 low
Relative risk significance	RAW	>2 significant importance
		>10 very safety severe >1,05 safety severe
	RRW - System level - Component level	 >1,05 significant importance >1,005 significant importance
	FV - System level - Component level	 >0,05 significant importance >0,005 significant importance

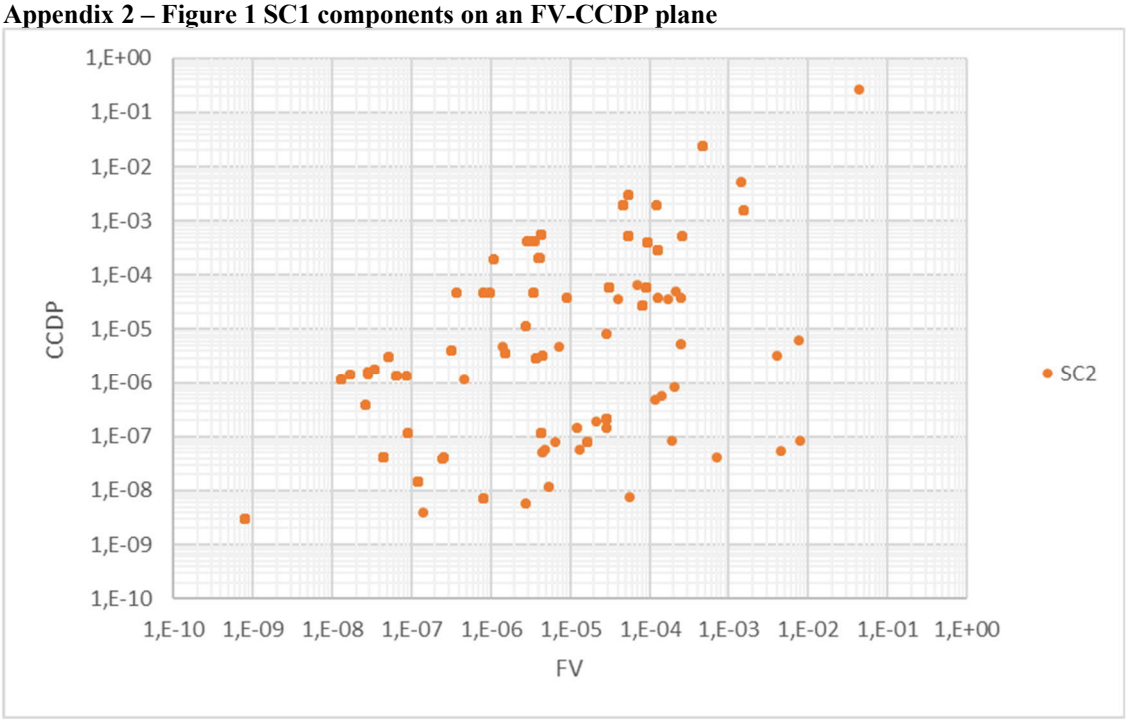
Appendix 1 – Table 2 Criteria for different levels of safety significance according to [70]

Risk Significance Ranking	Criteria
High safety significance	RAW ≥ 100,0 or FV ≥ 0,01 or FV ≥ 0,005 and RAW ≥ 2,0
Medium (further evaluation required)	FV < 0,005 and 100,0 > RAW ≥ 10,0
Medium safety significance	FV ≥ 0,005 and RAW < 2,0 or FV < 0,005 and 10,0 > RAW ≥ 2,0
Low safety significance	FV <0,005 and RAW < 2,0

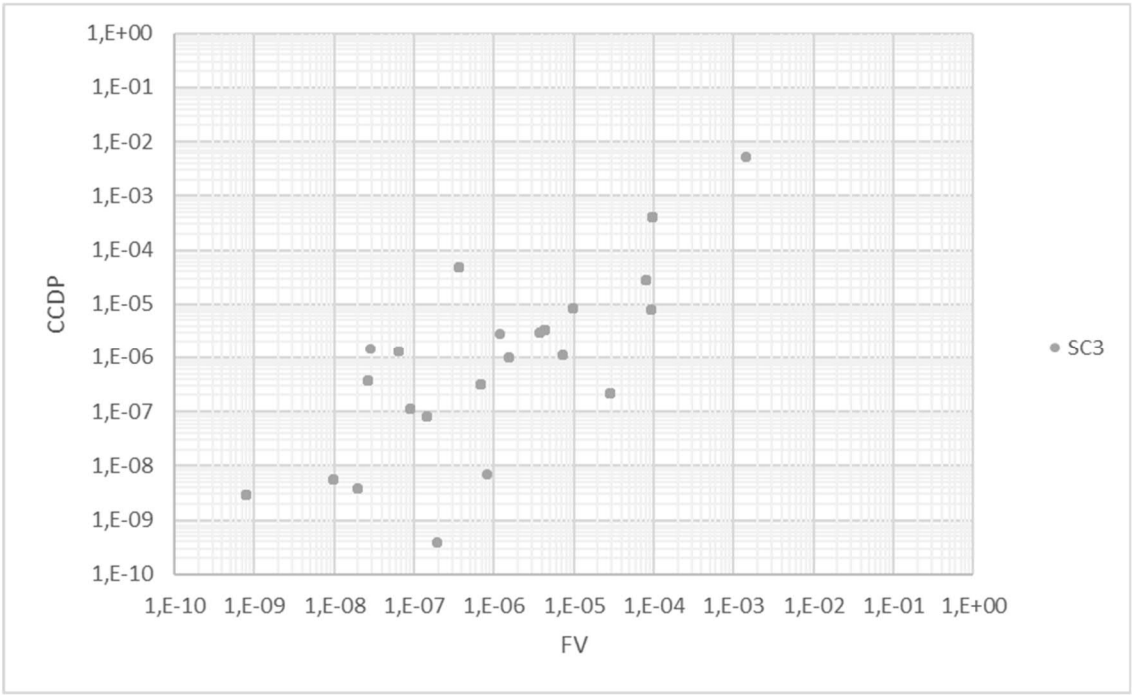
Appendix 2. FV-CCDP planes for different safety classes separately



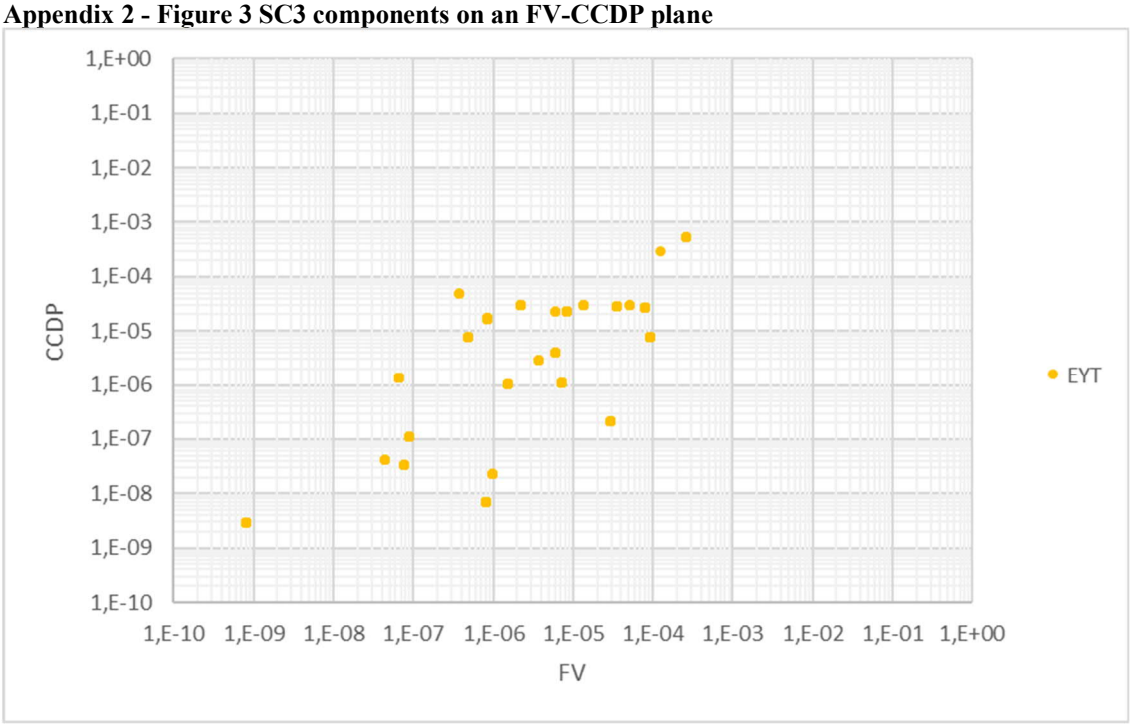
Appendix 2 – Figure 1 SC1 components on an FV-CCDP plane



Appendix 2 - Figure 2 SC2 components on an FV-CCDP plane

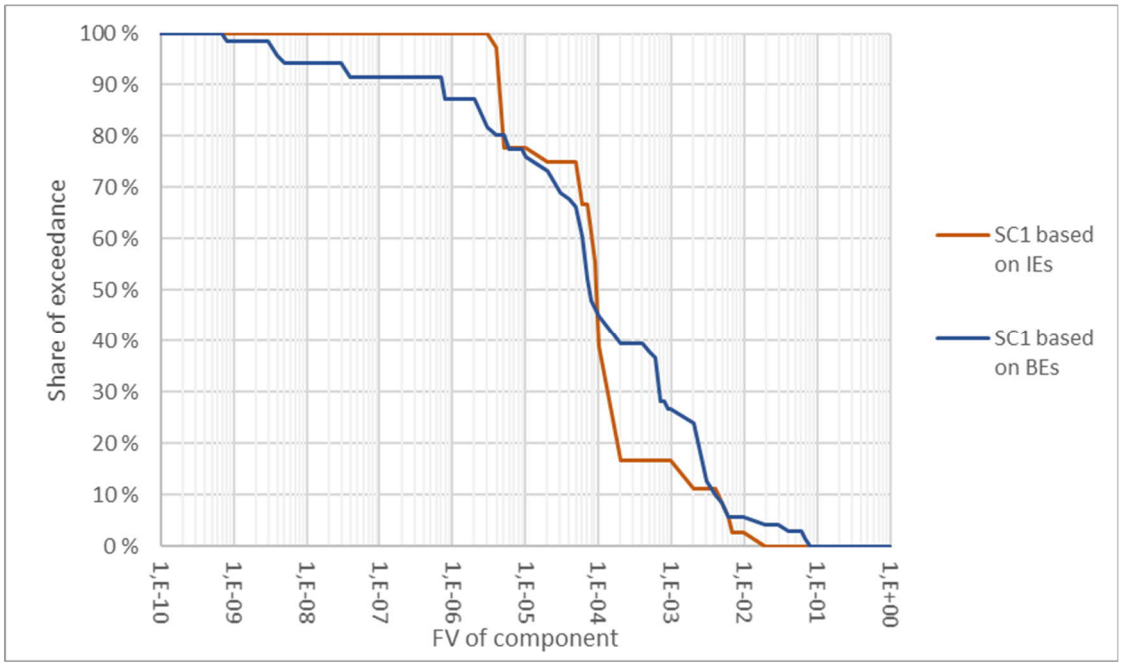


Appendix 2 - Figure 3 SC3 components on an FV-CCDP plane

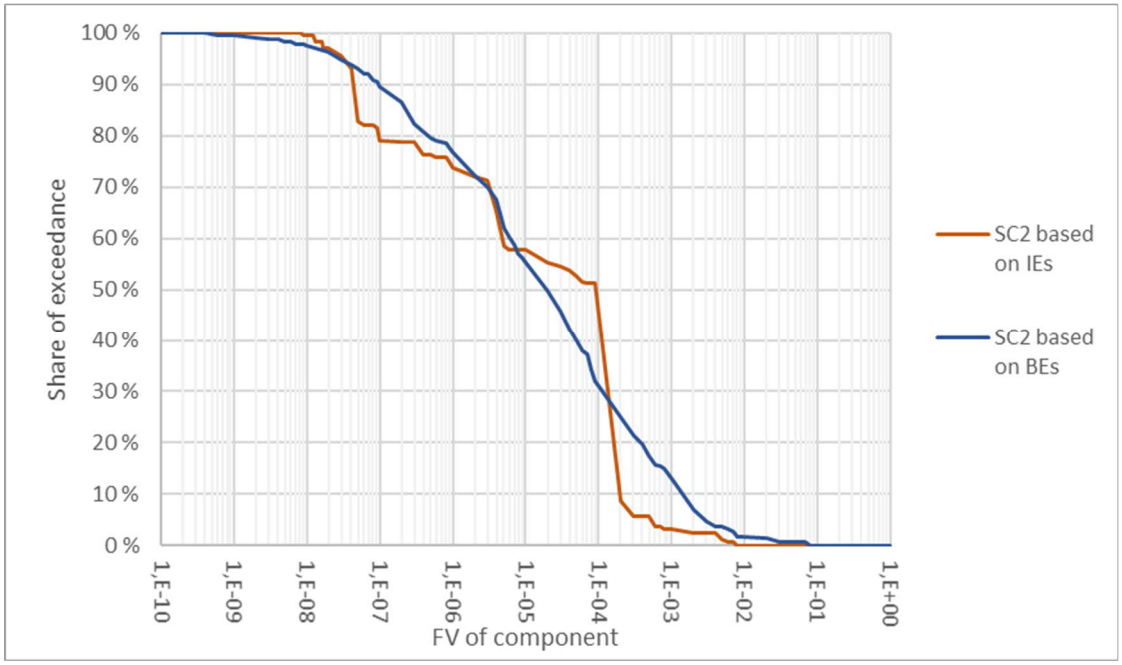


Appendix 2 - Figure 4 EYT components on an FV-CCDP plane

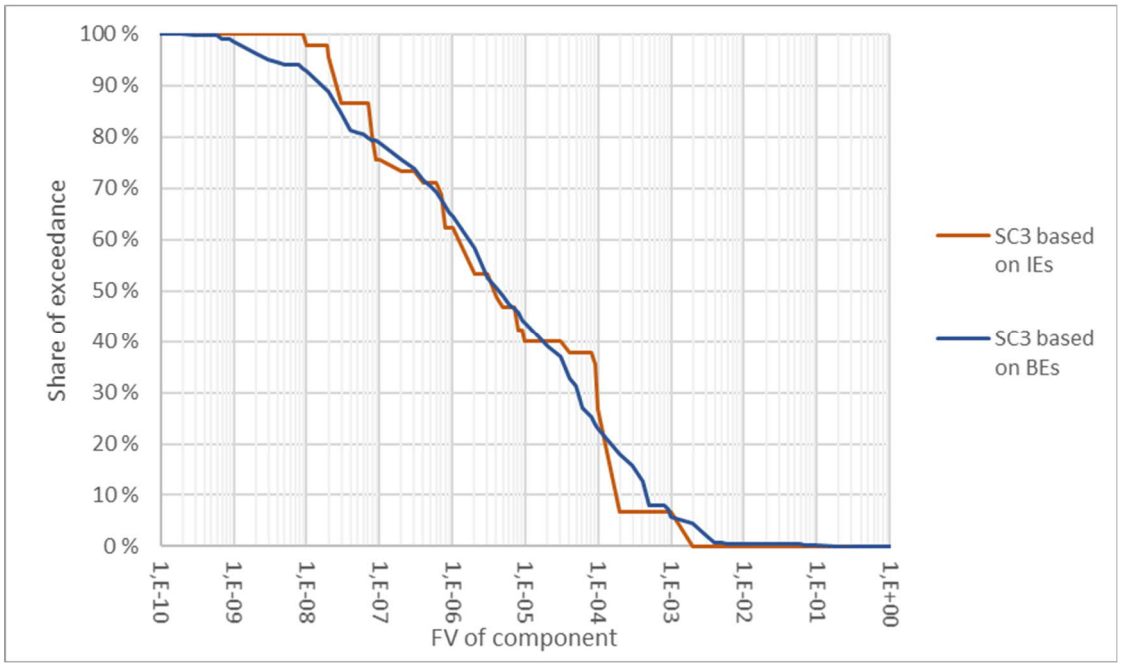
Appendix 3. Comparison between distributions of component level FV values calculated based on BEs and IEs



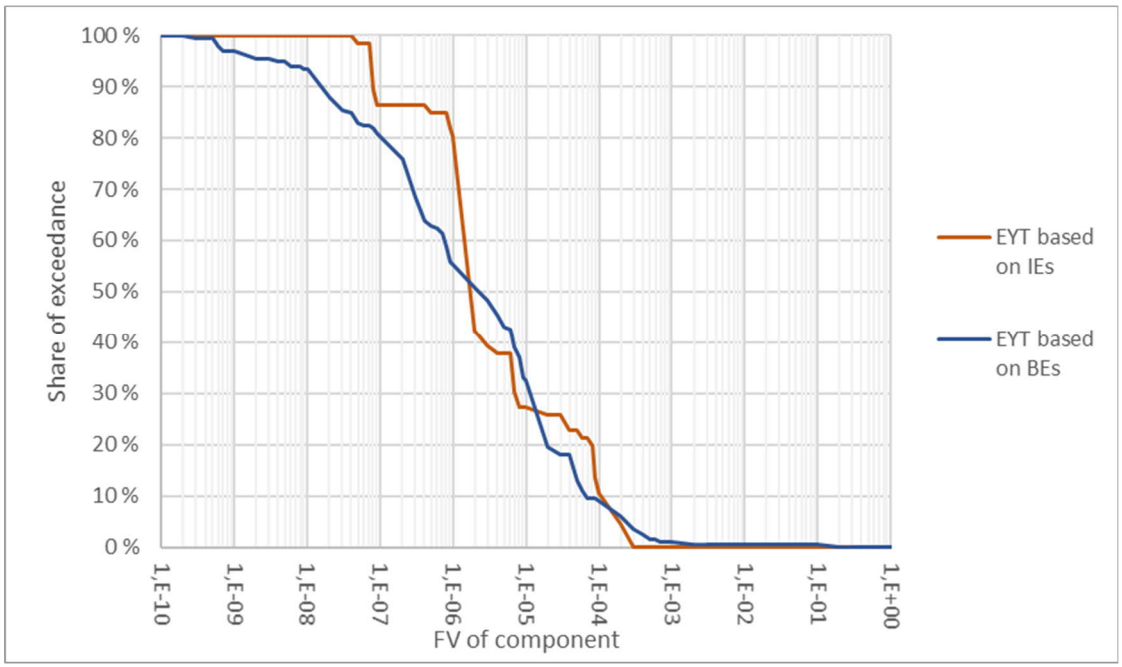
Appendix 3 – Figure 1 Distributions of component-level FV values of SC1 components calculated based on BEs and IEs separately



Appendix 3 – Figure 2 Distributions of component-level FV values of SC2 components calculated based on BEs and IEs separately



Appendix 3 – Figure 3 Distributions of component-level FV values of SC3 components calculated based on BEs and IEs separately



Appendix 3 – Figure 4 Distributions of component-level FV values of EYT components calculated based on BEs and IEs separately